VE6120K/VE6125K Virtual Appliances Installation Guide KVM Platform

Extreme Campus Controller™ Version 5.46.03

9037182-00 Rev AA
December 2021

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

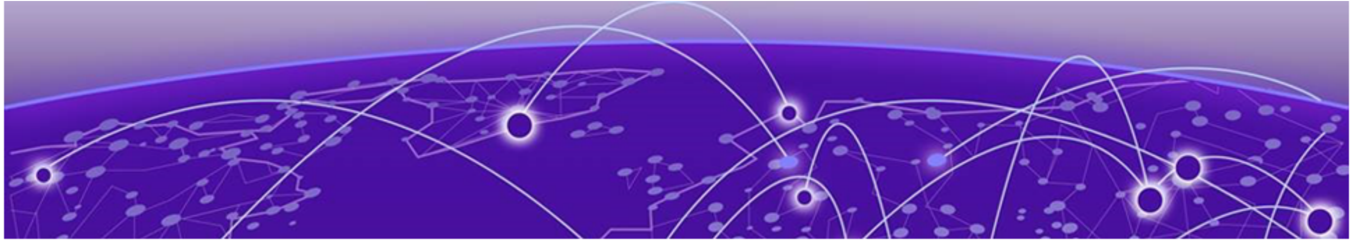
All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Table of Contents



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
💡	Tip	Helpful tips and notices for using the product
🗒	Note	Useful information or instructions
➡	Important	Important features or instructions
⚠	Caution	Risk of personal injury, system damage, or loss of data
⚠	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{` **`x`** `|` **`y`** `|` **`z`** `}`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x` `|` **`y`**	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *`member`*`[`*`member`*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, do either of the following:

- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

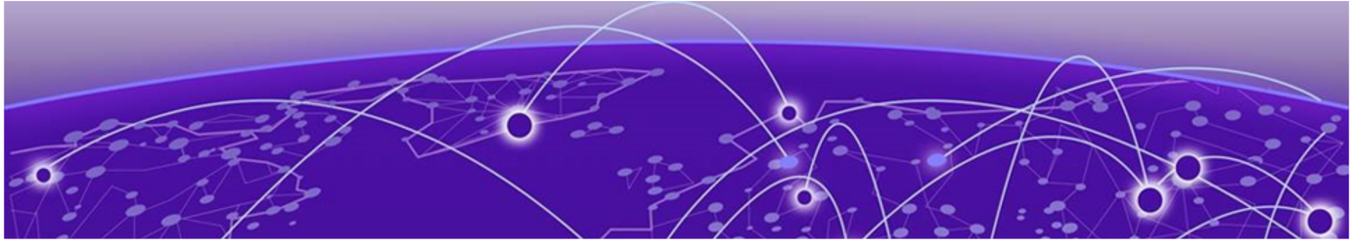
You can modify your product selections or unsubscribe at any time.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

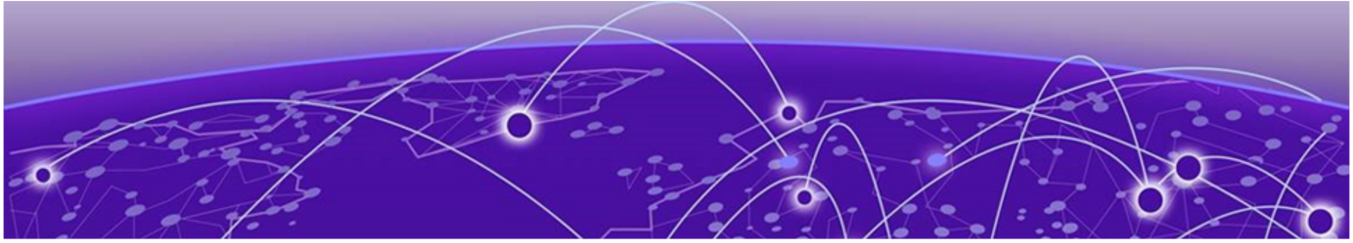


Overview

The guide describes how to configure and deploy the Extreme Campus Controller VE6120K and VE6125K Virtual Appliances. This guide is a reference for system administrators who install and manage the VE6120K and VE6125K Virtual Appliances.

Any administrator performing tasks described in this guide must have an account with administrative privileges.

> Note
> Different Linux distributions use different approaches to create and configure KVM virtual machines (VMs). This document will cover generic steps as well as specific examples for the Proxmox Virtual Environment (Proxmox VE) distribution.



Virtual Appliance Deployment

This section provides an overview of the requirements for the Extreme Campus Controller Virtual Appliances VE6120K and VE6125K deployments. It explains how to install the appliances on a KVM server.

Deployment Requirements

The VE6120K or VE6125K are distributed in the compressed raw disk images for the manually configured KVM virtual machine (VM). The appliances must be deployed on a KVM server host.

Note
VE6120K and VE6125K use separate deployment raw images. You cannot upgrade from VE6120K to VE6125K.

Note
You only need to deploy raw images when you first create the appliance VM. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a .dve file to the VE6120K appliance and .mfe file for the VE6125K appliance.

In addition, the appliances are configured with one Ethernet interface for administration and two data plane Ethernet interfaces for forwarding payload traffic.

The best practice is to connect them to separate bridges in the host server.

Configuration Options:

Table 4: Virtual Extreme Campus Controller (VE6120K and VE6125K)

Extreme Application	VE6120K			VE6125K
	Small	**Medium**	**Large**	**XLarge**
Total APs managed in Standalone mode	50	250	500	2000
Additional APs supported in high-availability mode	50	250	500	2000
Total managed APs per Appliance Pair	100	500	1000	4000

Table 4: Virtual Extreme Campus Controller (VE6120K and VE6125K) (continued)

Extreme Application	VE6120K			VE6125K
Total Switches managed per Appliance	50/100	100/200	200/400	200/400
Total simultaneous users in Standalone mode	1,000	4,000	8,000	16000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000	16000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000	32000
Hardware Requirements				
CPU	4	6	8	20 Cores
RAM (GB)	8	16	24	32
Hard Disk (GB)	80	80	80	250

- Consult KVM for minimum host performance requirements for virtual environment. Performance depends on network interface characteristics of underlying host and on utilization on shared interfaces by other virtual appliances.
- Host with 10 Gbps networking connections for data plane interfaces is recommended for best results on Large and XLarge VM profiles.

Connectivity Requirements

The appliances have one management interface (Admin) and two data plane interfaces (Port1, Port2).

Tip
The best practice is to connect to separate external bridges in the host.

The data plane interfaces have additional requirements on the bridges to which they connect:

- The bridge must accept promiscuous mode connections.
- The bridge must accept any VLAN tag traffic and forward it without changing or removing the VLAN tags.

Tip
The best practice is to configure the necessary bridges before installing the appliance.

For more information, see Configure Bridges for the Virtual Appliance for instructions on how to create and configure bridges that can be used by the Virtual Appliance's data plane ports.

Download a VE6120K/VE6125K Image

About This Task

Download the VE6120K-*.raw.xz/VE6125K-*.raw.xz software image to your host.

Procedure

1. Access the VE6120K/VE6125K download page at https://extremeportal.force.com/.
2. Download the image from **Downloads > Downloads Home** tab.
   a. Log into the **Downloads Home** using your Extreme Portal login credentials.
   b. Type VE6120K/VE6125K in the search tab and select the search icon. The image list is displayed.
   c. Download the **latest** VE6120K/VE6125K Virtual Appliance image.

Install and Deploy the Virtual Appliance Image - Generic Procedure

About This Task

To install the Virtual Appliance image using the generic procedure:

Procedure

1. Create a virtual machine based on the following parameters:

   - no CD-ROM device

   - OS: Linux, Version: 5.x - 2.6 Kernel

   - Machine: i440fx

   - BIOS: SeaBIOS

   - SCSI Controller: VirtIO SCSI

   - Disk size: 80GB (VE6120K) or 250GB (VE6125K)

   - Disk Cache: Write back

   - Video: none

   - CPU: host

   - Cores (socket 1): 4 (VE6120K Small), 6 (VE6120K Medium), 8 (VE6120K Large), or 20 (VE6125K XLarge)

   - Memory (MB): 8192 (VE6120K Small), 16384 (VE6120K Medium), 24576 (VE6120K Large), or 32768 (VE6125K XLarge)

   - Ballooning Device disabled

   - Network

   -- net0: Intel E1000, firewall disabled

   -- net1: VirtIO (paravirtualized), firewall disabled, multiqueue: 2 (VE6120K) or 4 (VE6125K)

   -- net2: VirtIO (paravirtualized), firewall disabled, multiqueue: 2 (VE6120K) or 4 (VE6125K)

   - Boot Order: scsi0

- serial console: -chardev socket, id=serial0, port=<console_port_number>, host=0.0.0.0, server, nowait, telnet -device isa-serial, chardev=serial0

- watchdog: -device 'i6300esb, bus=pci.0, addr=0×4'

Reference QEMU command line of the VE6120K Small VM:

```
/usr/bin/qemu-system-x86_64 \
  -id 104 \
  -name VE6120K \
  -no-shutdown \
  -chardev 'socket,id=qmp,path=/var/run/qemu-server/104.qmp,server,nowait' \
  -mon 'chardev=qmp,mode=control' \
  -chardev 'socket,id=qmp-event,path=/var/run/qmeventd.sock,reconnect=5' \
  -mon 'chardev=qmp-event,mode=control' \
  -pidfile /var/run/qemu-server/104.pid \
  -daemonize \
  -smbios 'type=1,uuid=c8cfd099-e370-4905-bf83-afa1e628c3ba' \
  -smp '4,sockets=1,cores=4,maxcpus=4' \
  -nodefaults \
  -boot 'menu=on,strict=on,reboot-timeout=1000,splash=/usr/share/qemu-server/
bootsplash.jpg' \
  -vga none \
  -nographic \
  -cpu host,+kvm_pv_eoi,+kvm_pv_unhalt \
  -m 8192 \
  -device 'pci-bridge,id=pci.1,chassis_nr=1,bus=pci.0,addr=0x1e' \
  -device 'pci-bridge,id=pci.2,chassis_nr=2,bus=pci.0,addr=0x1f' \
  -device 'vmgenid,guid=965377a1-862e-4bd4-94f2-96362dd522a7' \
  -device 'piix3-usb-uhci,id=uhci,bus=pci.0,addr=0x1.0x2' \
  -device 'usb-tablet,id=tablet,bus=uhci.0,port=1' \
  -device 'i6300esb,bus=pci.0,addr=0x4' \
  -iscsi 'initiator-name=iqn.1993-08.org.debian:01:c2a1f23f7fc1' \
  -device 'virtio-scsi-pci,id=scsihw0,bus=pci.0,addr=0x5' \
  -drive 'file=/storage/images/104/vm-104-disk-0.raw,if=none,id=drive-
scsi0,cache=writeback,format=raw,aio=threads,detect-zeroes=on' \
  -device 'scsi-hd,bus=scsihw0.0,channel=0,scsi-id=0,lun=0,drive=drive-
scsi0,id=scsi0,rotation_rate=1,bootindex=100' \
  -netdev 'type=tap,id=net0,ifname=tap104i0,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'e1000,mac=FE:22:F1:81:56:FF,netdev=net0,bus=pci.0,addr=0x12,id=net0' \
  -netdev 'type=tap,id=net1,ifname=tap104i1,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=06:B5:A9:CB:F3:2E,netdev=net1,bus=pci.0,addr=0x13,id=net1,vectors=6,mq=on' \
  -netdev 'type=tap,id=net2,ifname=tap104i2,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=E6:A3:20:1B:97:17,netdev=net2,bus=pci.0,addr=0x14,id=net2,vectors=6,mq=on' \
  -machine 'type=pc+pve0' \
  -chardev 'socket,id=serial0,port=56031,host=0.0.0.0,server,nowait,telnet' \
  -device 'isa-serial,chardev=serial0'
```

Reference QEMU command line of the VE6125K XLarge VM:

```
/usr/bin/qemu-system-x86_64 \
  -id 100 \
  -name VE6125K \
  -no-shutdown \
  -chardev 'socket,id=qmp,path=/var/run/qemu-server/100.qmp,server,nowait' \
  -mon 'chardev=qmp,mode=control' \
  -chardev 'socket,id=qmp-event,path=/var/run/qmeventd.sock,reconnect=5' \
  -mon 'chardev=qmp-event,mode=control' \
  -pidfile /var/run/qemu-server/100.pid \
  -daemonize \
  -smbios 'type=1,uuid=07cd719c-fc03-4d3d-ae36-4a612ebf21cf' \
  -smp '20,sockets=1,cores=20,maxcpus=20' \
  -nodefaults \
  -boot 'menu=on,strict=on,reboot-timeout=1000,splash=/usr/share/qemu-server/
bootsplash.jpg' \
  -vga none \
  -nographic \
  -cpu host,+kvm_pv_eoi,+kvm_pv_unhalt \
  -m 32768 \
  -device 'pci-bridge,id=pci.1,chassis_nr=1,bus=pci.0,addr=0x1e' \
  -device 'pci-bridge,id=pci.2,chassis_nr=2,bus=pci.0,addr=0x1f' \
  -device 'vmgenid,guid=42f181ea-8ffe-4d9b-ac0b-1f45ddb07698' \
  -device 'piix3-usb-uhci,id=uhci,bus=pci.0,addr=0x1.0x2' \
  -device 'usb-tablet,id=tablet,bus=uhci.0,port=1' \
  -device 'i6300esb,bus=pci.0,addr=0x4' \
  -iscsi 'initiator-name=iqn.1993-08.org.debian:01:c2a1f23f7fc1' \
  -device 'virtio-scsi-pci,id=scsihw0,bus=pci.0,addr=0x5' \
  -drive 'file=/dev/data2/vm-100-disk-0,if=none,id=drive-
scsi0,cache=writeback,format=raw,aio=threads,detect-zeroes=on' \
  -device 'scsi-hd,bus=scsihw0.0,channel=0,scsi-id=0,lun=0,drive=drive-
scsi0,id=scsi0,rotation_rate=1,bootindex=100' \
  -netdev 'type=tap,id=net0,ifname=tap100i0,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'e1000,mac=4E:FD:02:4C:C5:19,netdev=net0,bus=pci.0,addr=0x12,id=net0' \
  -netdev 'type=tap,id=net1,ifname=tap100i1,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=2A:39:7A:E0:8E:92,netdev=net1,bus=pci.0,addr=0x13,id=net1,vectors=10,mq=on' \
  -netdev 'type=tap,id=net2,ifname=tap100i2,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=56:5D:4A:16:63:AF,netdev=net2,bus=pci.0,addr=0x14,id=net2,vectors=10,mq=on' \
  -machine 'type=pc+pve0' \
  -chardev 'socket,id=serial0,port=56030,host=0.0.0.0,server,nowait,telnet' \
  -device 'isa-serial,chardev=serial0'
```

2. Upload the VE6120K-*.raw.xz/VE6125K-*.raw.xz deployment image obtained in Download a VE6120K/VE6125K Image on page 11 to the KVM server.
3. Uncompress the deployment image over the VM disk image.

   Depending on the selected or configured storage type, it could be a plain disk image file, a LVM storage, or a similar storage option. Check `-drive` parameter in the reference commands in the previous steps for more information.

   Sample commands to populate the disk locations from the examples provided in the previous steps:

   ```
   xz -dc VE6120K-06.01.01.0001.raw.xz > /storage/images/104/vm-104-disk-0.raw
   ```

   ```
   xz -dc VE6125K-06.01.01.0001.raw.xz | dd of=/dev/data2/vm-100-disk-0 bs=1M status=progress
   ```
4. Launch the prepared VM.

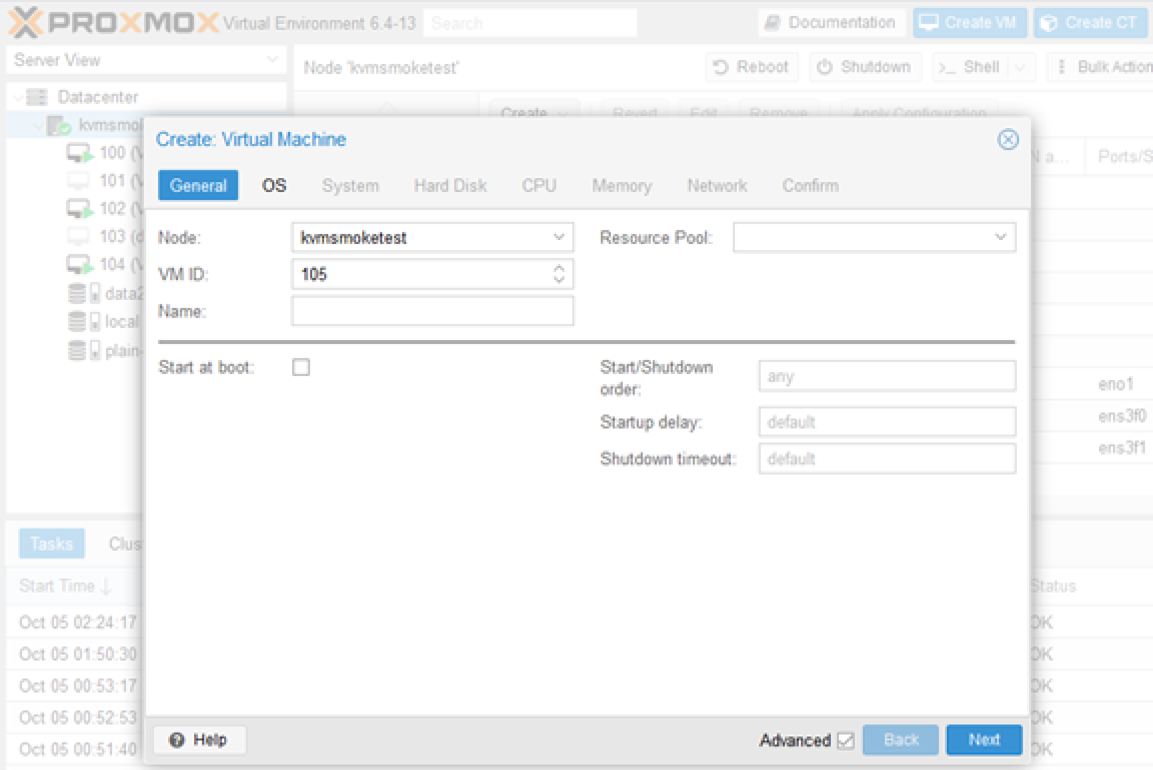
Install and Deploy the Virtual Appliance Image - Proxmox VE Procedure

About This Task

Create a virtual machine and configure the virtual machine settings. To install the Virtual Appliance image using the Proxmox VE procedure:

Procedure

1. Log into the Proxmox GUI.
2. In the left pane, select the KVM server host name.
3. Select **Create VM**.
4. Select **Advanced**.
5. Set the desired VM ID and select **Next**.



Node: kvmsmoketest

VM ID: 105

Name:

Resource Pool:

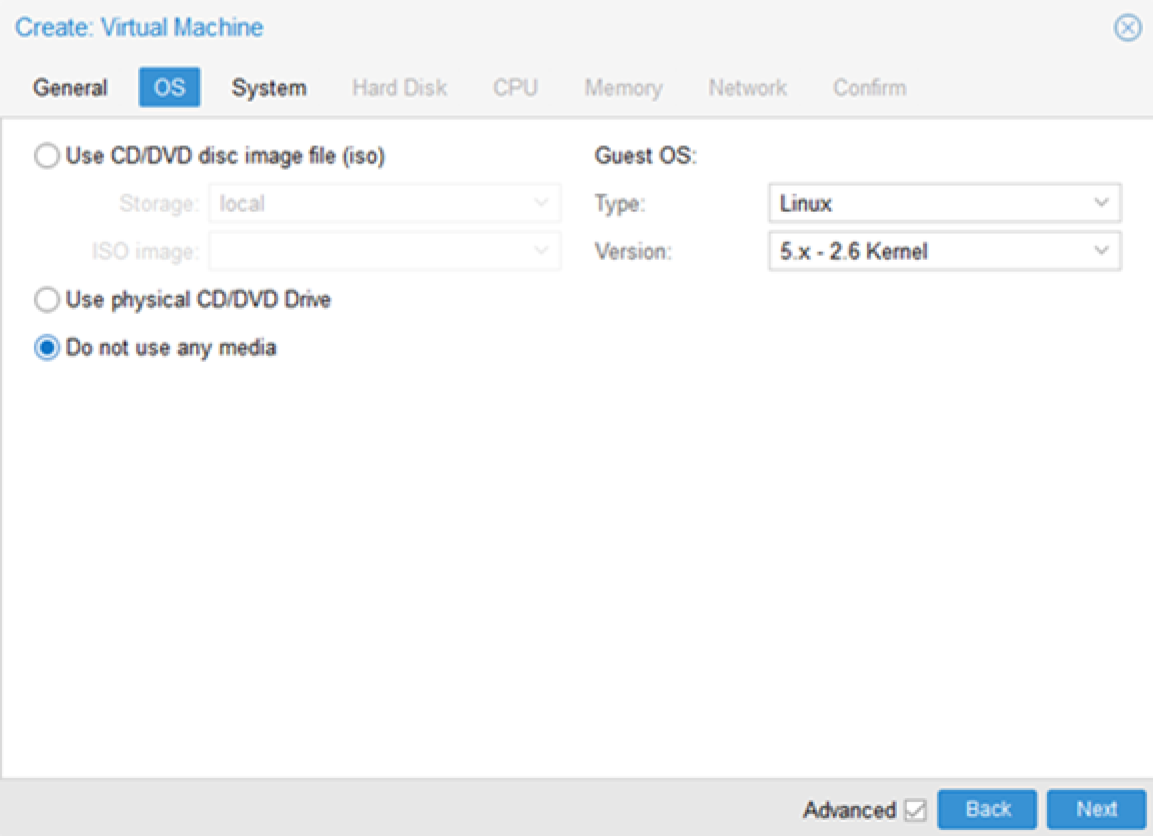
Start at boot: □

Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

6. Set the following **OS** configuration and select **Next**:
   a. Select **Do not use any media**.
   b. Set the Guest OS type to **Linux**.
   c. Set the Guest OS version to **5.x-2.6 Kernel**.


Create: Virtual Machine

○ Use CD/DVD disc image file (iso)

Storage: local

ISO image:

○ Use physical CD/DVD Drive

● Do not use any media

Guest OS:

Type: Linux

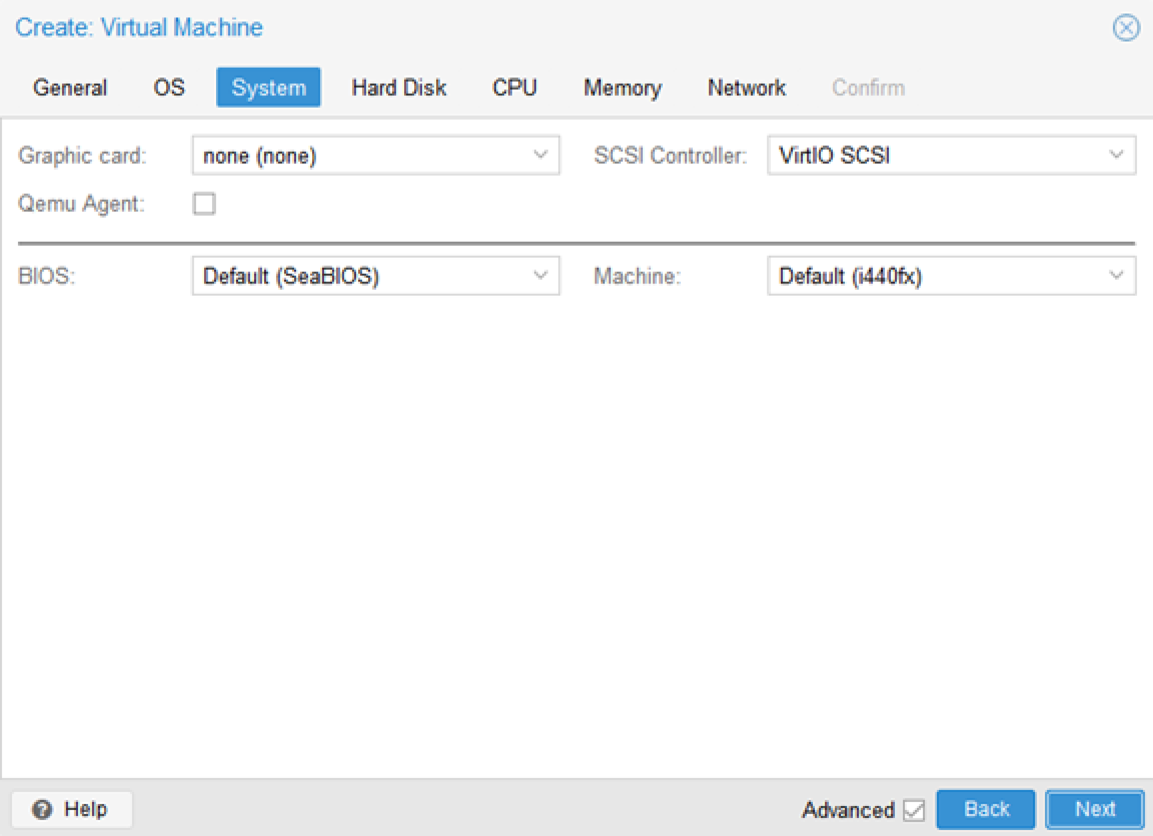
Version: 5.x - 2.6 Kernel

7. Set the following **System** configuration and select **Next**:

   a. Set the Graphic card option to **none**.

   b. Set the SCSI Controller to **VirtIO SCSI**.

   c. For Machine, select **`Default (i440fx)`**.



Graphic card: none (none)

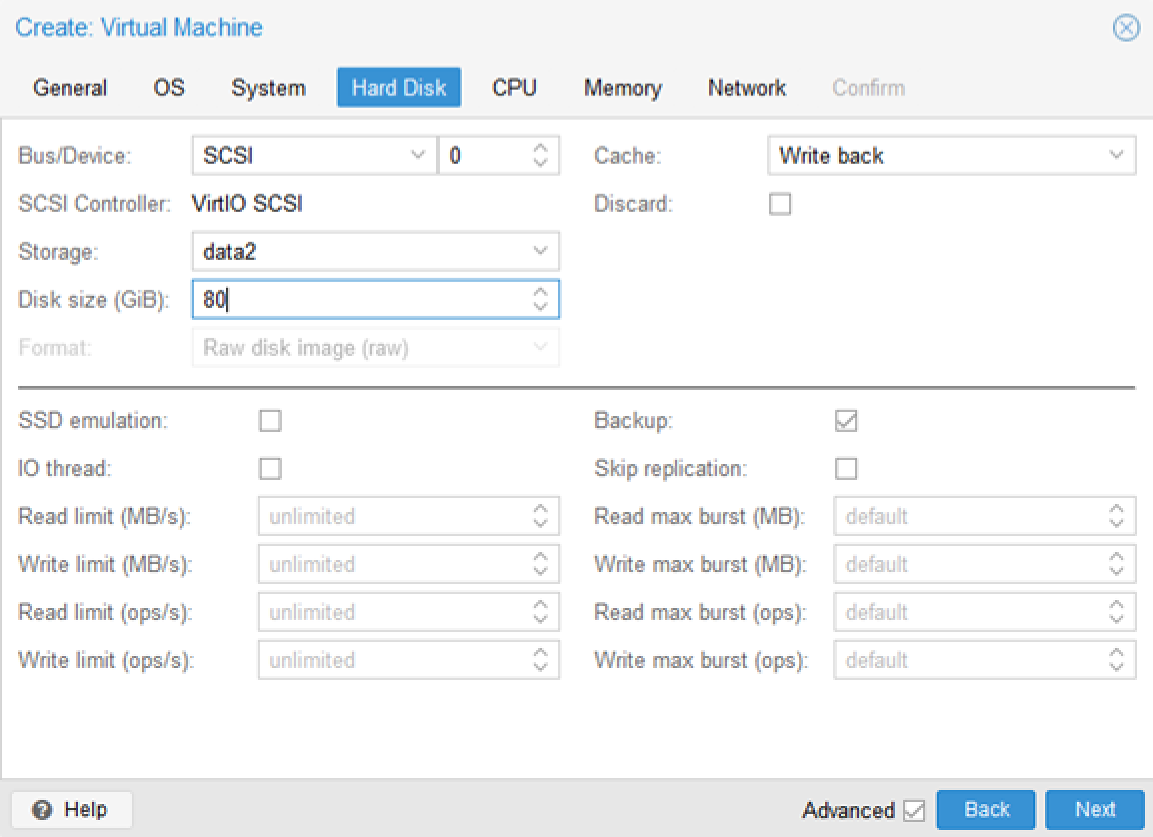
SCSI Controller: VirtIO SCSI

Qemu Agent: □

BIOS: Default (SeaBIOS)

Machine: Default (i440fx)

8. Select the appropriate storage available on the server.
9. Set the following **Hard Disk** configuration and select **Next**:
   a. Set the **Disk size (GB)** value to 80 for VE6120K and 250 for VE6125K.
   b. Set the disk image format to raw.
   c. Select **Write back** for Cache.
   d. Select **SSD emulation** if the corresponding storage on the server is SSD based.



Bus/Device: SCSI 0

SCSI Controller: VirtIO SCSI

Storage: data2

Disk size (GiB): 80

Format: Raw disk image (raw)

Cache: Write back

Discard: □

SSD emulation: □

IO thread: □

Read limit (MB/s): unlimited

Write limit (MB/s): unlimited

Read limit (ops/s): unlimited

Write limit (ops/s): unlimited

Backup: ☑

Skip replication: □

Read max burst (MB): default

Write max burst (MB): default

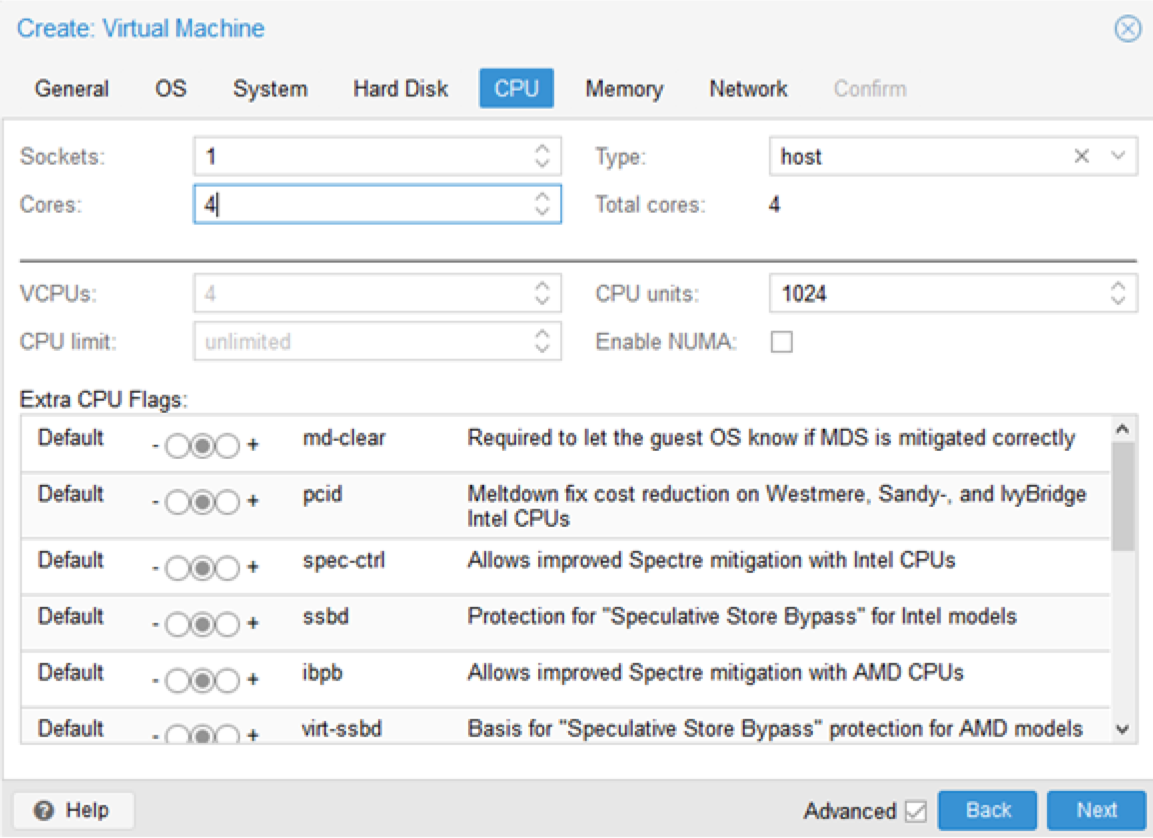
Read max burst (ops): default

Write max burst (ops): default

10. Set the following **CPU** configuration and select **Next**:

    a. Set the CPU type to **host**.

    b. Set the Cores to 4 for VE6120K Small, 6 for VE6120K Medium, 8 for VE6120K Large, and 20 for VE6125K XLarge (see Deployment Requirements on page 10 for reference).



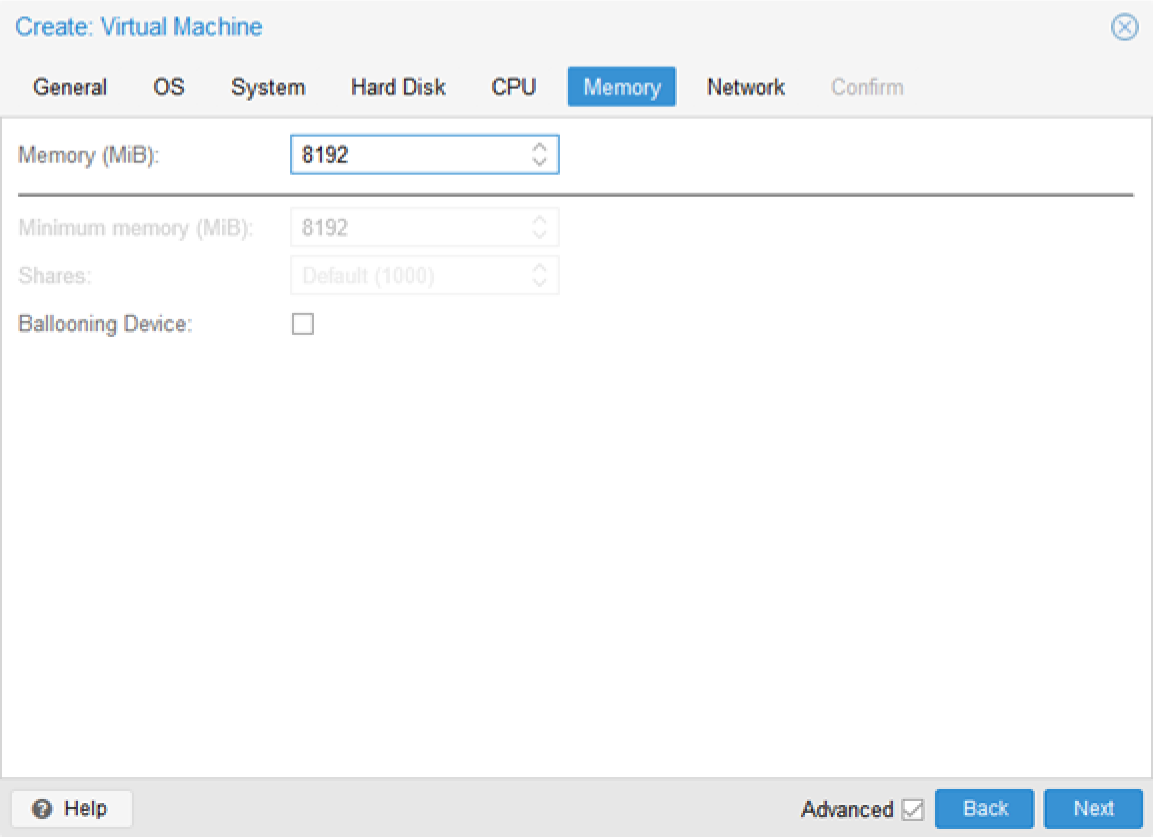
Sockets:	1	Type:	host
Cores:	4	Total cores:	4
VCPUs:	4	CPU units:	1024
CPU limit:	unlimited	Enable NUMA:	□

Extra CPU Flags:

Default	- ○●○ +	md-clear	Required to let the guest OS know if MDS is mitigated correctly
Default	- ○●○ +	pcid	Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs
Default	- ○●○ +	spec-ctrl	Allows improved Spectre mitigation with Intel CPUs
Default	- ○●○ +	ssbd	Protection for "Speculative Store Bypass" for Intel models
Default	- ○●○ +	ibpb	Allows improved Spectre mitigation with AMD CPUs
Default	- ○●○ +	virt-ssbd	Basis for "Speculative Store Bypass" protection for AMD models

11. Clear **Ballooning Device**. Set the following **Memory** configuration and select **Next**:

    Set the **Memory (MiB)** to 8192 for VE6120K Small, 16384 for VE6120K Medium, 24576 for VE6120K Large, and 32768 for VE6125K XLarge.



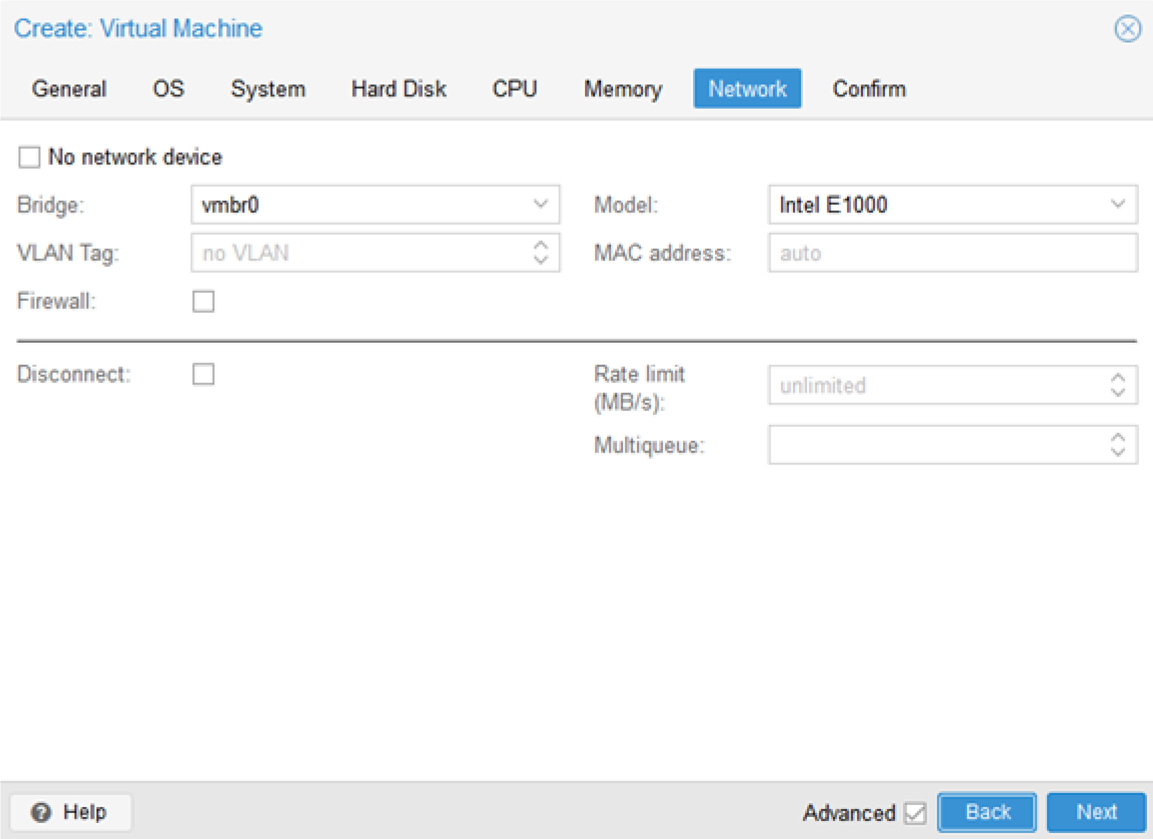
Memory (MiB): 8192

Minimum memory (MiB): 8192

Shares: Default (1000)

Ballooning Device: □

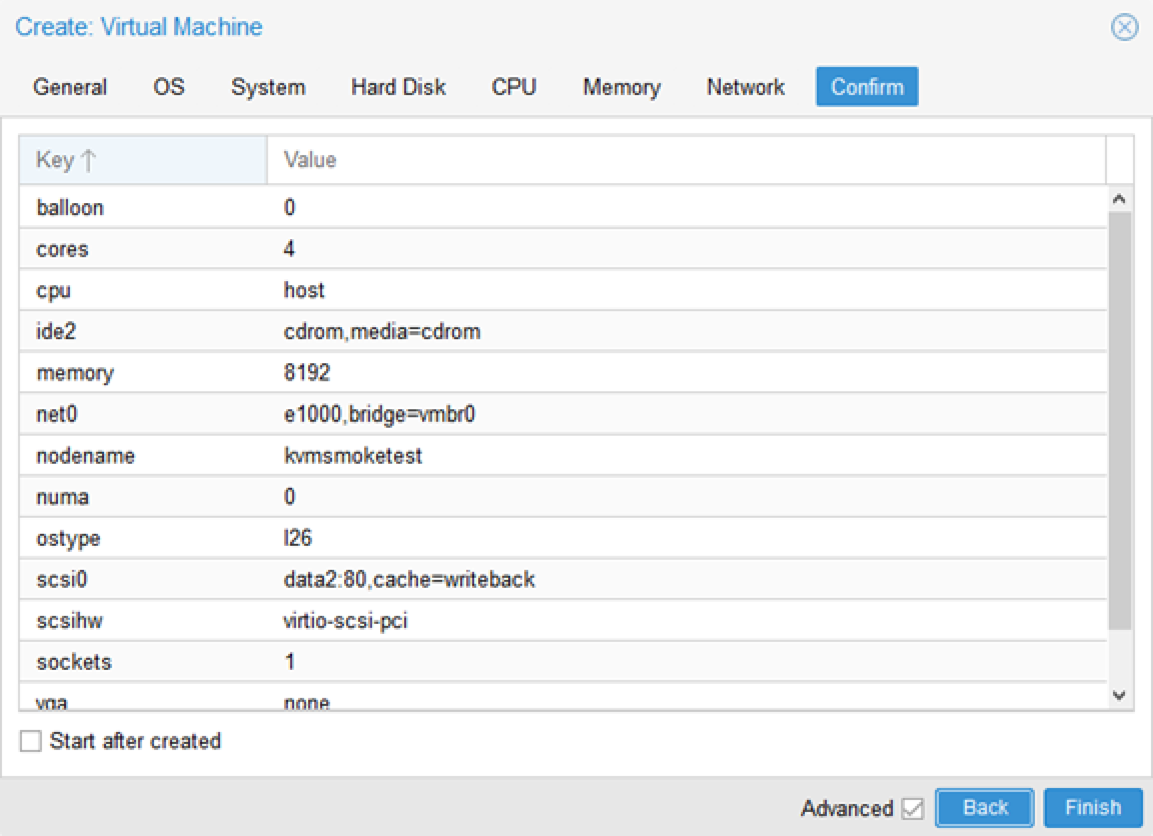
12. Set the following **Network** configuration and select **Next**:
    a. Select the Bridge for the Admin port.
    b. Set the **Model** as Intel E1000.
    c. Clear **Firewall**.


Create: Virtual Machine

□ No network device

Bridge:	vmbr0	Model:	Intel E1000
VLAN Tag:	no VLAN	MAC address:	auto
Firewall:	□		
Disconnect:	□	Rate limit (MB/s):	unlimited
		Multiqueue:	

13. Review the parameters and select **Finish**.



Key ↑	Value
balloon	0
cores	4
cpu	host
ide2	cdrom,media=cdrom
memory	8192
net0	e1000,bridge=vmbr0
nodename	kvmsmoketest
numa	0
ostype	l26
scsi0	data2:80,cache=writeback
scsihw	virtio-scsi-pci
sockets	1
vga	none

□ Start after created

Configure the Network Device

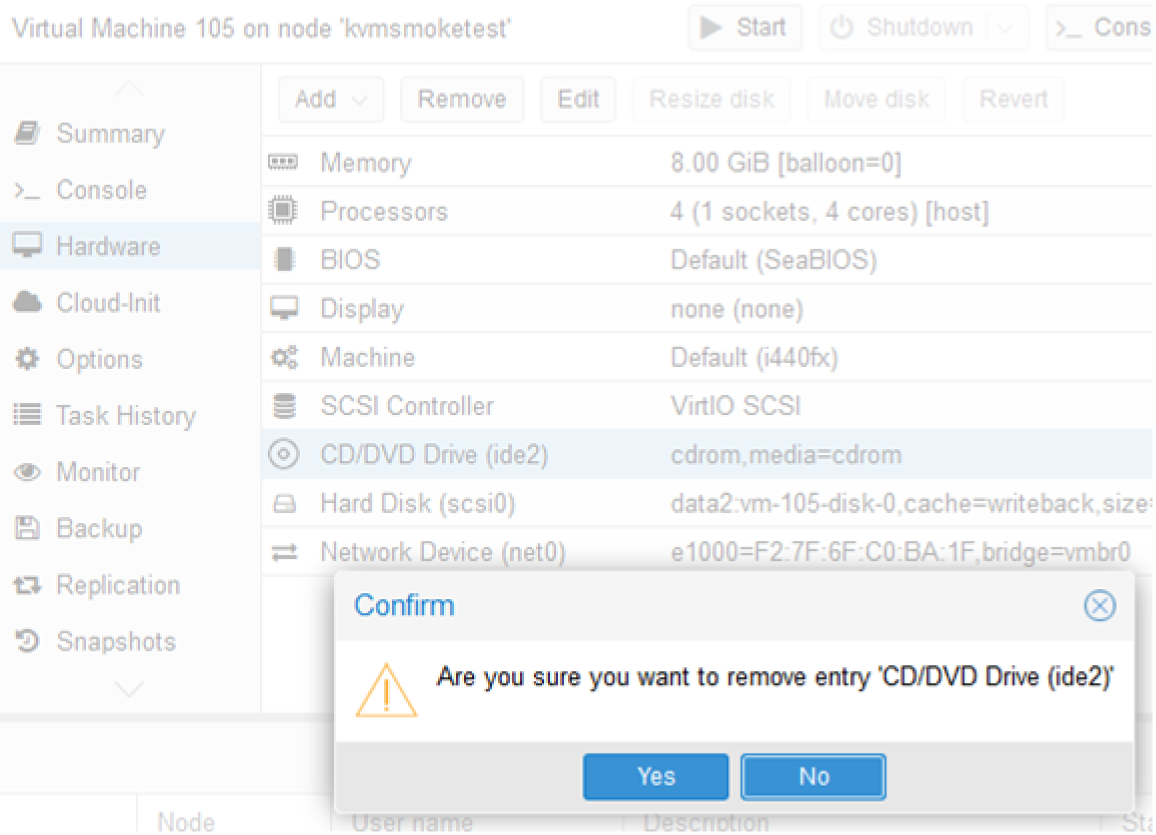
About This Task

After you create and configure the virtual machine initial setup, add and configure the network device. To configure a network device:

Procedure

1. Select the virtual machine that you created from the KVM server host name.
2. Select **Hardware**.
3. Select **CD/DVD Drive** > **Remove**.

4. Select **Yes** to confirm removing the CD/DVD Drive entry.



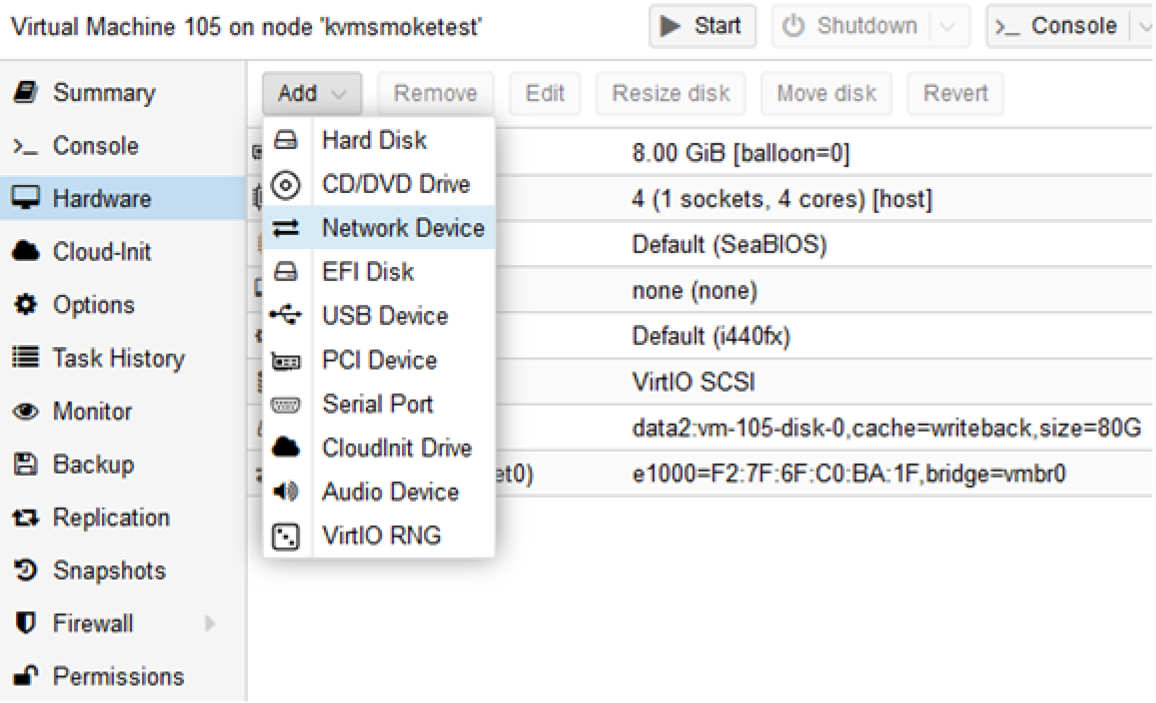
Virtual Machine 105 on node 'kvmsmoketest'

Memory	8.00 GiB [balloon=0]
Processors	4 (1 sockets, 4 cores) [host]
BIOS	Default (SeaBIOS)
Display	none (none)
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
CD/DVD Drive (ide2)	cdrom,media=cdrom
Hard Disk (scsi0)	data2:vm-105-disk-0,cache=writeback,size
Network Device (net0)	e1000=F2:7F:6F:C0:BA:1F,bridge=vmbr0

Confirm

Are you sure you want to remove entry 'CD/DVD Drive (ide2)'

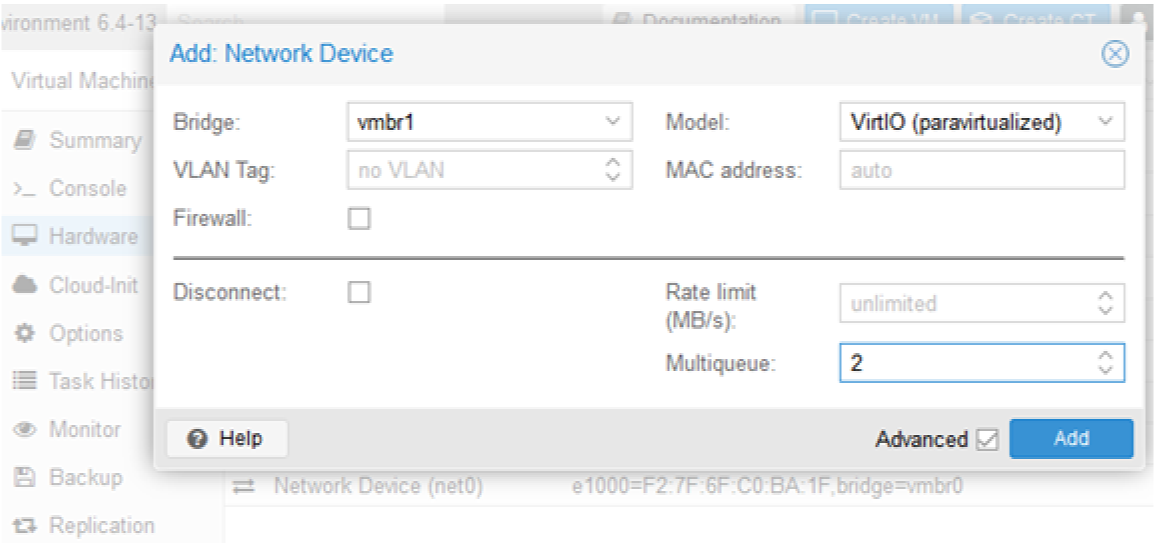
5. Select **Add** > **Network Device** to add data port interfaces.



Virtual Machine 105 on node 'kvmsmoketest'

	8.00 GiB [balloon=0]
	4 (1 sockets, 4 cores) [host]
	Default (SeaBIOS)
	none (none)
	Default (i440fx)
	VirtIO SCSI
	data2:vm-105-disk-0,cache=writeback,size=80G
et0)	e1000=F2:7F:6F:C0:BA:1F,bridge=vmbr0

6. Configure the following **Add: Network Device** settings:
   a. Set the Bridge for the first data port interface.
   b. Set the model to **VirtIO (paravirtualized)**.
   c. Clear **Firewall**.
   d. Set Multiqueue to **2** for VE6120K and to **4** for VE6125K.

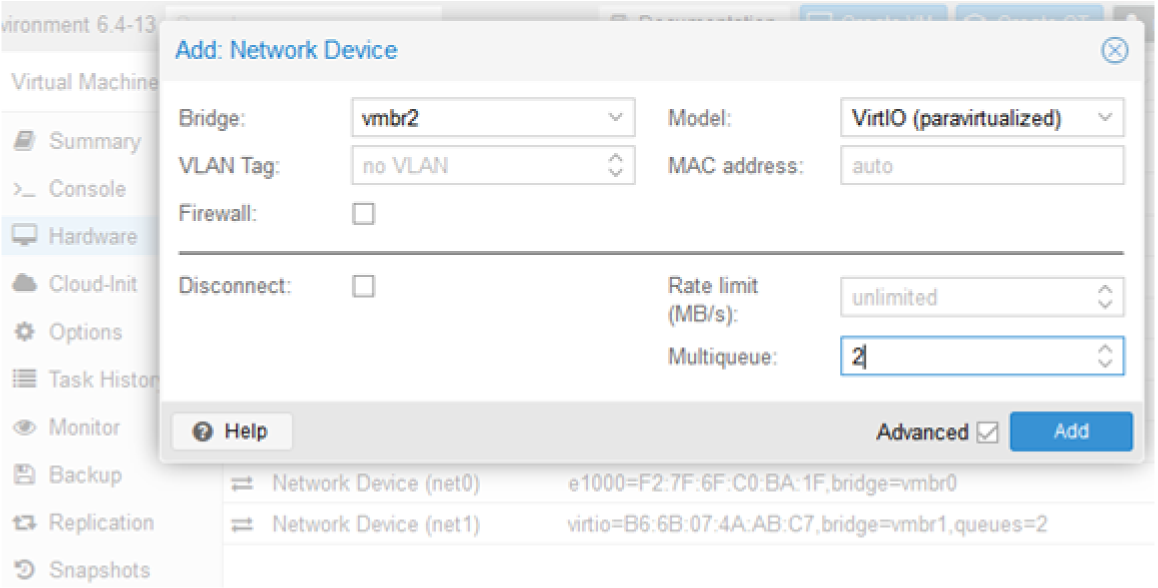


Add: Network Device

Bridge: vmbr1
Model: VirtIO (paravirtualized)
VLAN Tag: no VLAN
MAC address: auto
Firewall: □
Disconnect: □
Rate limit (MB/s): unlimited
Multiqueue: 2
Advanced ☑

Network Device (net0) e1000=F2:7F:6F:C0:BA:1F,bridge=vmbr0

   e. Select **Add**.
7. Select **Bridge** for the second data port interface and configure the other values as described in the previous step.

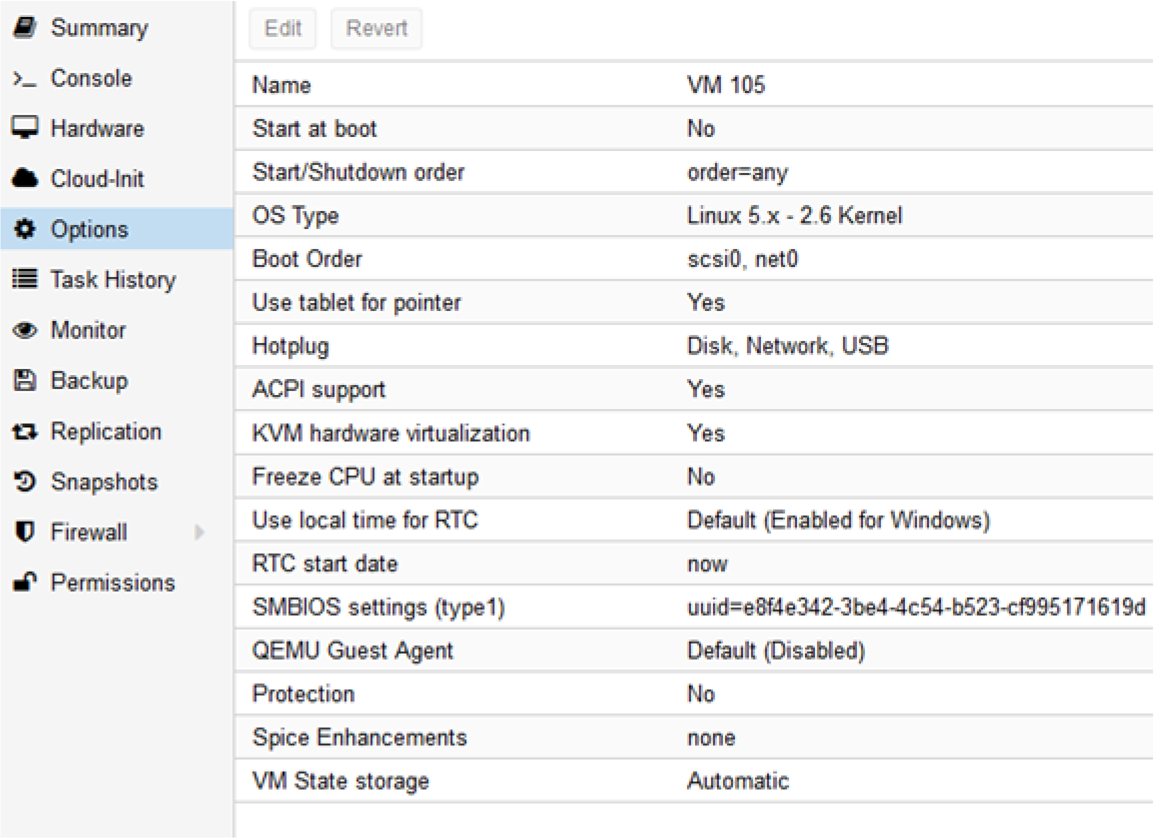


Add: Network Device

Bridge: vmbr2
Model: VirtIO (paravirtualized)
VLAN Tag: no VLAN
MAC address: auto
Firewall: □
Disconnect: □
Rate limit (MB/s): unlimited
Multiqueue: 2
Advanced ☑

Network Device (net0) e1000=F2:7F:6F:C0:BA:1F,bridge=vmbr0
Network Device (net1) virtio=B6:6B:07:4A:AB:C7,bridge=vmbr1,queues=2

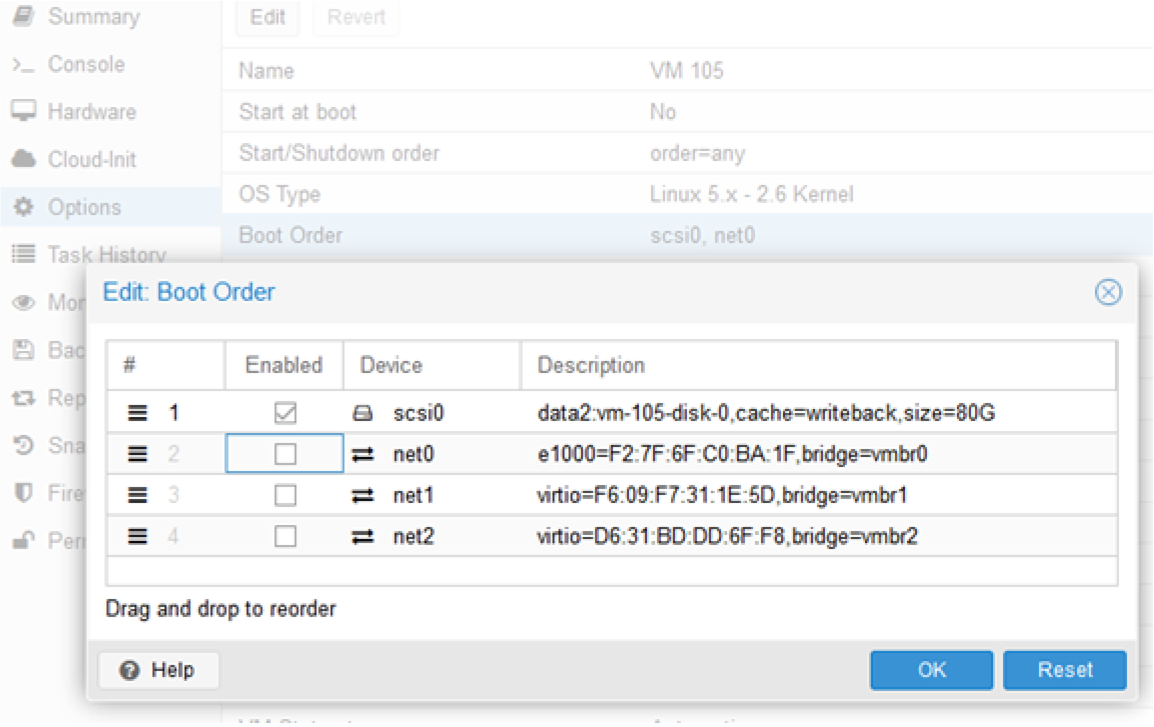
8. Select **Options**.



Name	VM 105
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 5.x - 2.6 Kernel
Boot Order	scsi0, net0
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
KVM hardware virtualization	Yes
Freeze CPU at startup	No
Use local time for RTC	Default (Enabled for Windows)
RTC start date	now
SMBIOS settings (type1)	uuid=e8f4e342-3be4-4c54-b523-cf995171619d
QEMU Guest Agent	Default (Disabled)
Protection	No
Spice Enhancements	none
VM State storage	Automatic

9. Select **Boot Order** > **Edit**.

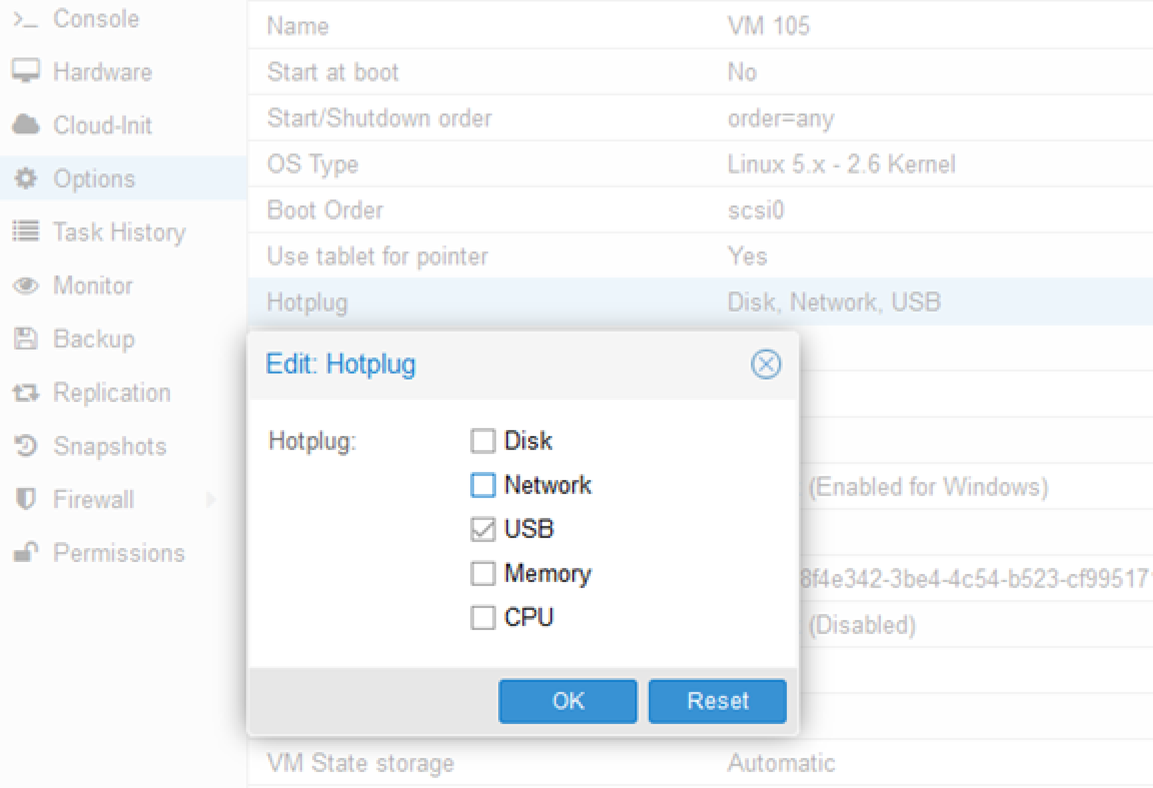
10. Clear all the edit options except **scsi0**, and select **OK**.



#	Enabled	Device	Description
1	☑	scsi0	data2:vm-105-disk-0,cache=writeback,size=80G
2	□	net0	e1000=F2:7F:6F:C0:BA:1F,bridge=vmbr0
3	□	net1	virtio=F6:09:F7:31:1E:5D,bridge=vmbr1
4	□	net2	virtio=D6:31:BD:DD:6F:F8,bridge=vmbr2

Drag and drop to reorder

11. Select **Hotplug** > **Edit**.
12. Clear all the edit options except **USB**, and select **OK**.



Name	VM 105
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 5.x - 2.6 Kernel
Boot Order	scsi0
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
VM State storage	Automatic

Edit: Hotplug

Hotplug: ☐ Disk ☐ Network ☑ USB ☐ Memory ☐ CPU

Launch the Virtual Machine

About This Task

Perform the following steps to successfully launch a virtual machine. To launch a VM:

Procedure

1. Log into the Proxmox server using secure shell (SSH).
2. Edit the virtual machine configuration file using the following details:

   The virtual machine configuration file is located under `/etc/pve/nodes/<KVM_hostname>/qemu-server/<VM_ID>.conf`, where **KVM_hostname** is the name of the server and **VM_ID** is the virtual machine ID number configured in Step 4.

   Edit the VM configuration file to add the following two lines to add serial port and watchdog functionality:

   ```
   args: -chardev
   socket,id=serial0,port=<console_port_number>,host=0.0.0.0,server,nowait,telnet -device
   isa-serial,chardev=serial0
   watchdog: i6300esb
   ```

   The serial port is added and configured for network access on a network port specified in the `<console_port_number>`.

   VE6120K Small Proxmox VM configuration file (e.g. <VM_ID>.conf) sample:

   ```
   # cat /etc/pve/nodes/KVMSERVER/qemu-server/102.conf
   args: -chardev socket,id=serial0,port=56028,host=0.0.0.0,server,nowait,telnet -device
   ```

```
isa-serial,chardev=serial0
balloon: 0
boot: order=scsi0
cores: 4
cpu: host
hotplug: usb
memory: 8192
name: VE6120K
net0: e1000=BA:44:BE:F7:AA:08,bridge=vmbr0
net1: virtio=E2:55:A7:86:0D:FF,bridge=vmbr1,queues=2
net2: virtio=52:AA:44:EB:DC:A0,bridge=vmbr2,queues=2
numa: 0
ostype: l26
scsi0: plain-storage:102/vm-102-disk-0.raw,cache=writeback,size=80G,ssd=1
scsihw: virtio-scsi-pci
smbios1: uuid=7a25ec0b-0d9f-4fde-9fe4-821afa5f396f
sockets: 1
vga: none
vmgenid: 8013433b-e9ed-4249-9604-2c5ebf0a4b74
vmstatestorage: data2
watchdog: i6300esb
```

VE6125K XLarge Proxmox VM configuration file sample:

```
# cat /etc/pve/nodes/KVMSERVER/qemu-server/100.conf
args: -chardev socket,id=serial0,port=56030,host=0.0.0.0,server,nowait,telnet -device
isa-serial,chardev=serial0
balloon: 0
boot: order=scsi0
cores: 20
cpu: host
hotplug: usb
memory: 32768
name: VE6125K
net0: e1000=4E:FD:02:4C:C5:19,bridge=vmbr0
net1: virtio=2A:39:7A:E0:8E:92,bridge=vmbr1,queues=4
net2: virtio=56:5D:4A:16:63:AF,bridge=vmbr2,queues=4
numa: 0
ostype: l26
scsi0: data2:vm-100-disk-0,cache=writeback,size=250G,ssd=1
scsihw: virtio-scsi-pci
smbios1: uuid=07cd719c-fc03-4d3d-ae36-4a612ebf21cf
sockets: 1
vga: none
vmgenid: 42f181ea-8ffe-4d9b-ac0b-1f45ddb07698
vmstatestorage: data2
watchdog: i6300esb
```

3. Upload the obtained deployment image (VE6120K-*.raw.xz or VE6125K-*.raw.xz) to the KVM server.
4. Uncompress the deployment image over the VM disk image.

   Depending on the selected or configured storage type, it could be a plain disk image file, a LVM storage, or a similar storage option.

   Use the following example to find the image location:

   qm showcmd **<VM_ID>** --pretty | grep \\-drive

```
# qm showcmd 105 --pretty | grep \\-drive
  -drive 'file=/dev/data2/vm-105-disk-0,if=none,id=drive-
scsi0,cache=writeback,format=raw,aio=threads,detect-zeroes=on' \

# qm showcmd 102 --pretty | grep \\-drive
  -drive 'file=/storage/images/102/vm-102-disk-0.raw,if=none,id=drive-
scsi0,cache=writeback,format=raw,aio=threads,detect-zeroe\
```

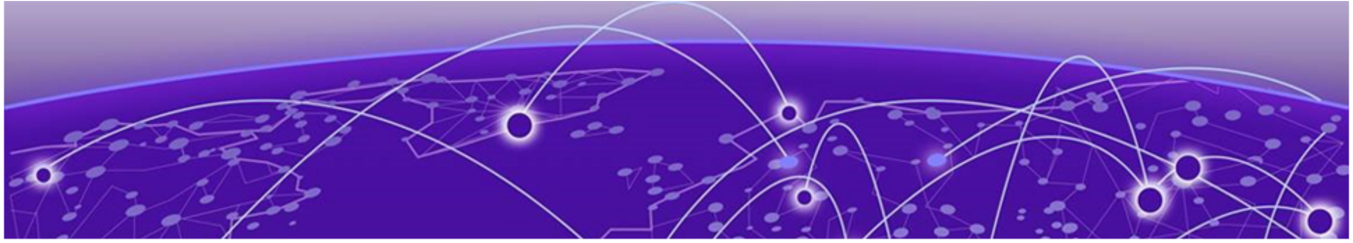
Use the following commands to populate the disk locations from the previously mentioned examples:

```
xz -dc VE6125K-06.01.01.0001.raw.xz | dd of=/dev/data2/vm-100-disk-0 bs=1M
status=progress

xz -dc VE6120K-06.01.01.0001.raw.xz > /storage/images/102/vm-102-disk-0.raw
```

The VM is ready to launch.

5. On the Proxmox UI, select **VM** > **Start** to launch the VM.



Virtual Appliance Configuration

After the Virtual Appliance has been deployed on a KVM server using the instructions in Virtual Appliance Deployment on page 10 you are ready to perform initial server configuration.

Access the Virtual Appliance Console

About This Task

To log in to the Virtual Appliance and perform the initial configuration, access the VM console as follows:

Procedure

1. During VM creation, the VM serial port is configured for network access on a particular port.

   To access the console over telnet:

   ```
   telnet <kvm_server_ip> <console_port_number>
   ```

   <kvm_server_ip> is the IP address of the KVM server and **<console_port_number>** is the serial port from the VM serial port configuration.

   Example: telnet 10.0.0.2 55555
2. Type your login credentials:
   - For **User Name**, type admin.
   - For **Password**, type abc123.

   You now are working in the VE6120K's CLI.

   ```
   root@host:~# telnet 10.0.0.2 55555
   Trying 10.0.0.2...
   Connected to 10.0.0.2.
   Escape character is '^]'.

   Extreme Campus Controller version 06.01.01.0001
   Unauthorized access is prohibited.
   VE6120K.extremenetworks.com login:
   ```

   To end the telnet session, press Ctrl-], and type **quit**.

Configure the VE6120K/VE6125K Using the Basic Configuration Wizard

The Extreme Campus Controller software provides a Basic Configuration Wizard that can help administrators configure the minimum settings necessary to deploy a fully functioning VE6120K/VE6125K appliance on a network.

Administrators can use the wizard to quickly configure the appliances for deployment, and then after the installation is complete, continue to revise the configuration accordingly.

The wizard is automatically launched when an administrator logs on to the VE6120K/VE6125K CLI for the first time, including after the system has been reset to the factory default settings.

The configuration wizard prompts with a set of **Yes** or **No** questions. The default value is indicated in parenthesis. To accept the default value, press **Enter**.

For more information about using the Basic Configuration Wizard, see Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard on page 30.

Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard

About This Task

After logging into the CLI of the VE6120K/VE6125K Basic Configuration Wizard, you will be able to set it up using a set of **Yes** or **No** commands.

Procedure

1. After logging into the CLI of VE6120K/VE6125K, you will be prompted to change the admin password. To begin the admin password setup, press **Enter**.

   The **Admin password Configuration** window opens.

   a. To change the password for the admin account, press **Enter**.
   b. Type the new password for the admin account.

      Note
      The password must be between 8 to 24 characters.

   c. Repeat the new password for the admin account and press **Enter**.

      If the passwords match, the password is accepted.
   d. Press **Enter** to accept the changes.

      The **AP access password** window opens.
2. To reset the AP access password, type a new password in the CLI.

   Note
   The password must be between 5 to 30 alphanumeric characters and can include period, dash, underscore, and space.

   a. Retype the AP access password. Select **Enter**.

      Your AP access password is now reset and the **Current Data Port Settings** CLI opens.

Current Data Port Settings

About This Task

When you set up the **Admin Password configuration**, you will be prompted to set up the **Current Data Port Settings**. To set up the data port:

Procedure

1. In the **Current Data Port Settings**, you will determine the port settings. The default port is **Port1**.
2. Select **Enter** to select **Port1**.
3. Set IP Address to the default value. The default value is **`10.0.0.1`**.
4. Press **Enter**.

   The IP Address is selected.
5. Set Netmask to default value of **`255.255.255.0`**.
6. Press **Enter**.

   The Netmask is set.
7. Press **Enter** to set the default VLAN. The tagged frames command opens.
8. Press **Enter** to keep the default tagged frames value to **`No`**.
9. To enable management on the interface, press **Enter** to select the default value, **`Yes`**.
10. To enable device registration, press **Enter** to select the default value, **`yes`**. The updated Data Port Interface settings open.

11. To accept the changes and keep the data port settings to the values you have chosen, press **Enter**.

    The Data Port Interface is now set. The CLI navigates to the **Current Host Attributes Settings** window.

Current Host Attributes

About This Task

To set up the current host attributes:

Procedure

1. Press **Enter** to change the Host Attributes.
2. Press **Enter** to enter the host name for the application.
3. Type **Y** to set up a dedicated Admin port for out-of-band management. The default option is `no`.

   The following note opens: Admin port does not allow device registration.
4. Type the IP address in the following format `xx.xx.xx.xx` to set up the IP address for the Admin Port.
5. Press **Enter** to accept the default IP netmask for the Admin Port.
6. Press **Enter** to accept the default domain name for the appliance. The default domain name is `extremenetworks.com`.
7. Press **Enter** to configure your Primary DNS server.
8. Type another IP address `xx.xx.xx.xx` to set up the IP address of the Primary DNS and press **Enter**.
9. The default option to set up a Secondary DNS server is `no`. Press **Enter** to accept the default option.

   The updated Host Attribute settings are displayed. To accept the changes you have made, press **Enter**. The **Current Global Default Gateway Settings** CLI opens.

Current Global Default Gateway Settings

About This Task

The global default gateway can be on any Admin or data port topology or subnet.

Procedure

1. Type an IP address.
2. Press **Enter** to accept the changes.

   You are navigated to the **Current Time Settings** CLI.

Current Time Settings

About This Task

The Current Time Settings option allows you to change the time zone as per your location.

Procedure

1. Press **Enter** to change the Time settings.

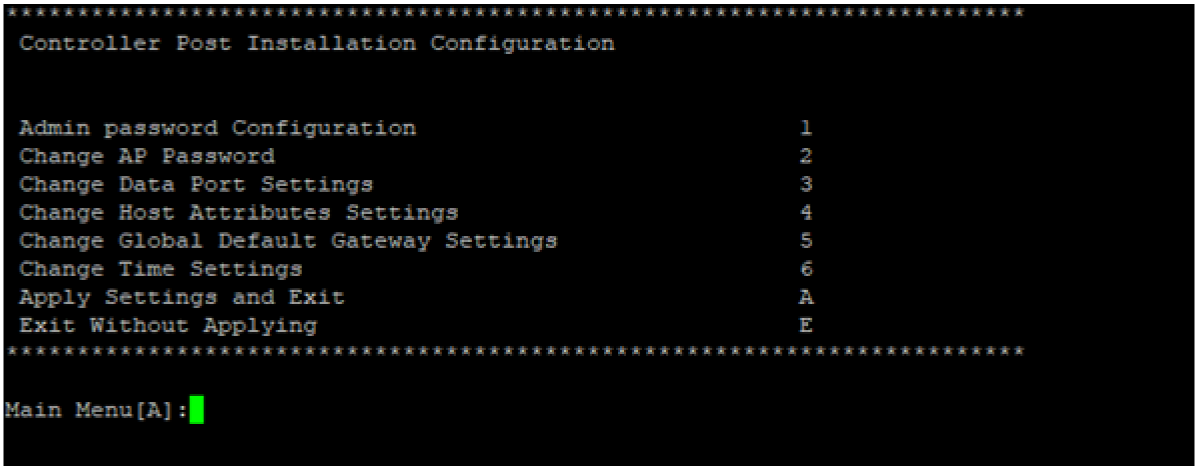
2. Press **Enter** again if you would like to change the Time Zone. The Region number list is displayed.

   > Important
   > Ensure that Extreme Campus Controller is configured with the correct Network Time Protocol (NTP) Server settings. Licensing management and several other system functions are dependent on an accurate timestamp. Configure NTP settings on Extreme Campus Controller during the initial setup wizard or alternatively under **Administration** > **System** > **Network Time** (as a first configuration step).

3. Pick a number according to the region numbers that is displayed on screen to pick you continent. Then, enter a number that corresponds to the Region. You can enter `n` to move down the list, or `p` to move up the list. To go back to the Region selection, press `c`.
4. Press **Enter** to run NTP as a client.
5. Provide the fully qualified domain name of the NTP server.
6. Press **Enter**.
7. You are prompted to enter a second NTP server and the default option is `y`. Type `n` and press **Enter**.

   NTP Client is enabled.
8. Accept the changes you have made to the time zone and NTP server by pressing **Enter**.

   You are navigated to the **Controller Post Installation Configuration** window along with the menu.
9. If you want to revisit any of the previous windows or exit without applying the configuration changes, enter one of the corresponding numbers or alphabets displayed on screen.



```
************************************************************************
 Controller Post Installation Configuration


 Admin password Configuration                                   1
 Change AP Password                                             2
 Change Data Port Settings                                      3
 Change Host Attributes Settings                                4
 Change Global Default Gateway Settings                         5
 Change Time Settings                                           6
 Apply Settings and Exit                                        A
 Exit Without Applying                                          E
************************************************************************

Main Menu[A]:
```

Figure 1: Controller Post Installation Configuration Menu

Table 5: Controller Post Installation Configuration Menu

Menu Option	Command
Admin password Configuration	1
Change AP Password	2
Change Data Port Settings	3
Change Host Attribute Settings	4
Change Global Default Gateway Settings	5

Table 5: Controller Post Installation Configuration Menu (continued)

Menu Option	Command
Change Time Settings	6
Apply Settings and Exit	A
Exit Without Applying	E

When you revisit any other screen, you will have to reconfigure all subsequent area settings. For example, if you decide to reconfigure the Admin Password, which is at the beginning of the configuration wizard, you will have to reconfigure all the subsequent configuration wizard settings.

Press **Enter** to accept the settings. The default option for accepting the settings is **A**. Your settings are now applied successfully.

Upgrade the VE6120K/VE6125K Software

About This Task

If you are not installing the latest Extreme Campus Controller release, you need to upgrade the VE6120K/VE6125K software to the latest patch release.

Procedure

1. Go to the Extreme Networks Support site and download the most recent Extreme Campus Controller software patch.
2. Log in to the virtual appliance using the admin user and password that you configured in the Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard on page 30 section.

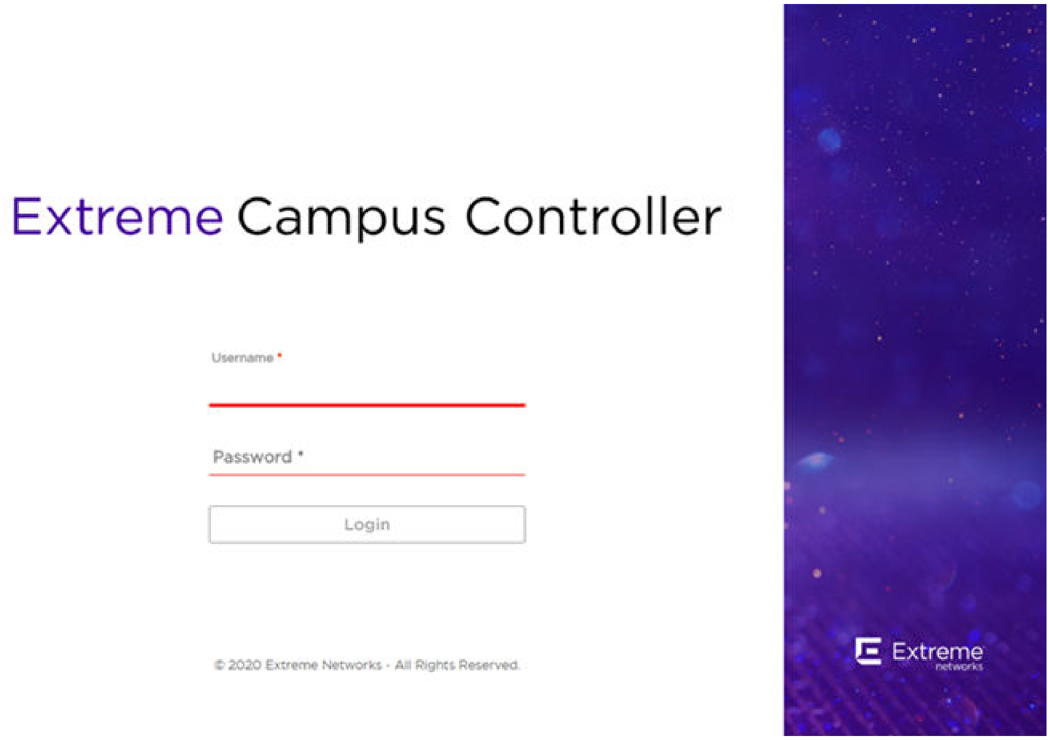
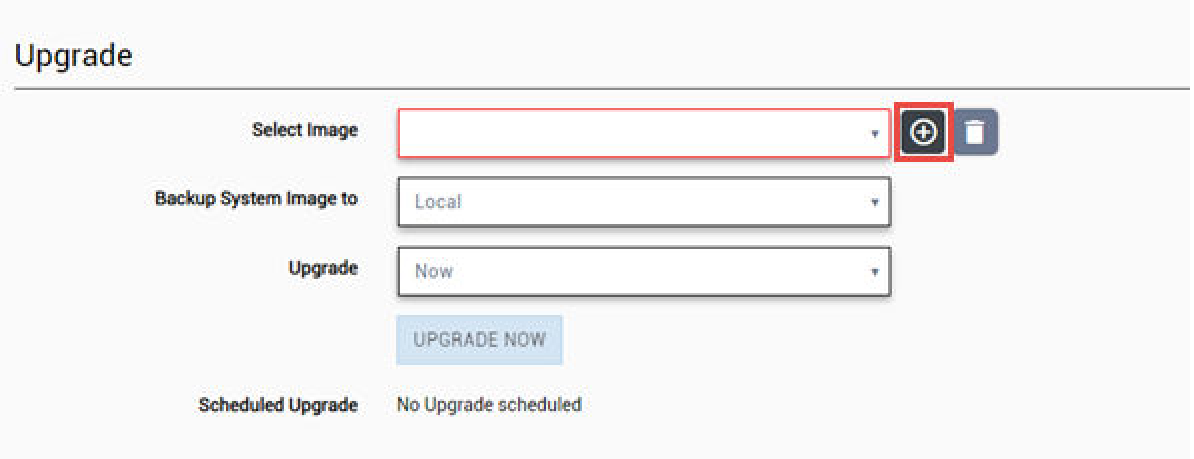

Extreme Campus Controller
Username *
Password *
Login
© 2020 Extreme Networks - All Rights Reserved.
Extreme networks

Figure 2: Virtual Appliance Login Window

3. Go to **Administration > System**.

   The **System** window is displayed.
4. Select **Software Upgrade** tab, and navigate to the **Upgrade** section.
5. To add the image file, select the plus icon.



Upgrade

Select Image:

Backup System Image to: Local

Upgrade: Now

Scheduled Upgrade: No Upgrade scheduled

Figure 3: Upgrade section

The **Copy Upgrade Image** window is displayed.

6. To copy an upgrade or backup image to Extreme Campus Controller, configure the following parameters:

   Image Type

   Indicates the type of image file used. Valid values are:

   - Upgrade
   - Backup

   Destination

   Destination of the uploaded image file:

   - Local
   - Flash (The Flash drive must be mounted.)

   Upload Method

   Method used to upload image file to appliance. Valid values are:

   - HTTP — Indicates to upload from a local workstation.
   - FTP — Indicates to upload from the corresponding server.
   - SCP — Indicates to upload from the corresponding server.

   When the Upload Method is **FTP** or **SCP**, configure the server properties.

   Copy Image from Local Drive

   When the Upload Method is **HTTP**, drag image onto Extreme Campus Controller or select field to navigate to local file directory.

   Select Image

   Due to a storage space limitation, Extreme Campus Controller limits the number of locally available upgrade images. If necessary, you can delete an older image before you upgrade to the latest image. To delete an image from Extreme Campus Controller, from the **Select Image** field, select an image and select 🗑.

What to Do Next

For more information about the **Software Upgrade** options, see the Extreme Campus Controller User Guide.

Perform a Backup

The backup and restore procedure is limited to configuration files and, optionally, logs and audit files. A system backup is a full system snapshot rescue file (*-rescue-user.tgz). Creating a rescue file is an option during the system upgrade process. For more information on system upgrade, see Upgrade the Virtual Appliance Software.

Before you perform a backup procedure, decide what to backup and where to save the backup file:

- Select back up configs, logs, and audit or back up configuration only.
- Select a location to store the backup file.
- (Optional) Configure a backup schedule.

On-demand backups can only be stored locally, while scheduled backups can be stored on a mounted flash drive or on a remote server.

Copy Backup

To copy a backup image to Extreme Campus Controller, configure the following parameters:

Upload Method

Method used to upload file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto Extreme Campus Controller or select field to navigate to local file directory.

Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Generic Procedure

Before You Begin

Prepare the Virtual Appliance to accept USB flash drives. The VM must be shut down before adding the USB flash drive.

1. Format the flash drive to FAT32.

2. Insert the flash drive into a USB port on the host.

   Note
   A USB device is required to be plugged in before it can be added to a virtual machine.

About This Task

The Virtual Appliance can accept USB flash drives. The flash drive can be used for backing up, restoring, upgrading, and collecting log information.

To add a USB flash drive to a shutdown VM:

Procedure

1. Log in to the host using a CLI (for example, SSH) to run the following command:

```
# lsusb
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 004: ID 1604:10c0 Tascam
Bus 003 Device 003: ID 1604:10c0 Tascam
Bus 003 Device 002: ID 1604:10c0 Tascam
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 002: ID 0424:5744 Standard Microsystems Corp. Hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 125f:c08a A-DATA Technology Co., Ltd. C008 Flash Drive
```

2. Extend your VM configuration:

   To add the flash drive using USB vendor or device ID:

   Note
   Adjust the addr field depending on the devices that are already defined on the PCI bus.

```
-device 'nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b'
-device 'usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0'
```

   Note
   vendorid and productid arguments need to match the flash drive ID from the lsusb output.

   To add the flash drive using the USB port:

```
-device 'nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b'
-device 'usb-host,bus=xhci.0,hostbus=1,hostport=1.3,id=usb0'
```

   Note
   hostbus and hostport arguments need to match the flash drive bus and device numbers from the lsusb output.

3. Start the VM.

Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Proxmox VE Procedure

Before You Begin

Prepare the Virtual Appliance to accept USB flash drives. The VM must be shut down before adding the USB flash drive.

1. Format the flash drive to FAT32.
2. Insert the flash drive into a USB port on the host.

Note

A USB device is required to be plugged in before it can be added to a virtual machine.

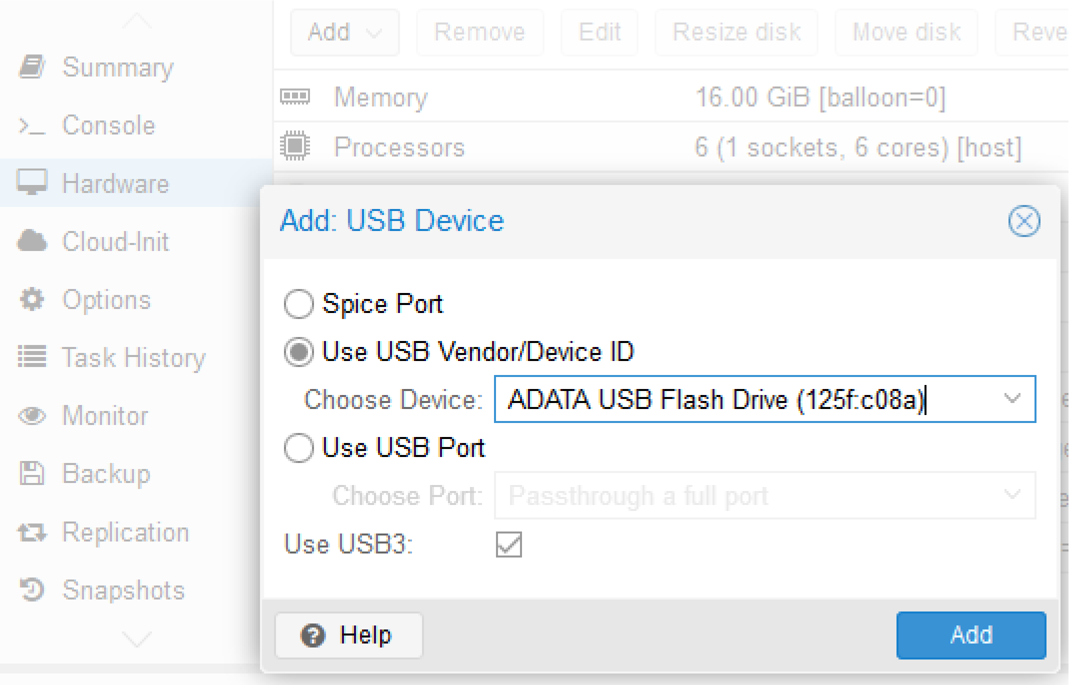
About This Task

The Virtual Appliance can accept USB flash drives. The flash drive can be used for backing up, restoring, upgrading, and collecting log information.

To add a USB flash drive to a shutdown VM:

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Hardware**.
4. Select **Add** > **USB Device**.
    a. To add a flash drive using USB vendor or device ID, select **Use USB Vendor/Device ID**, and choose a device.



Memory 16.00 GiB [balloon=0]

Processors 6 (1 sockets, 6 cores) [host]

Add: USB Device

○ Spice Port

● Use USB Vendor/Device ID

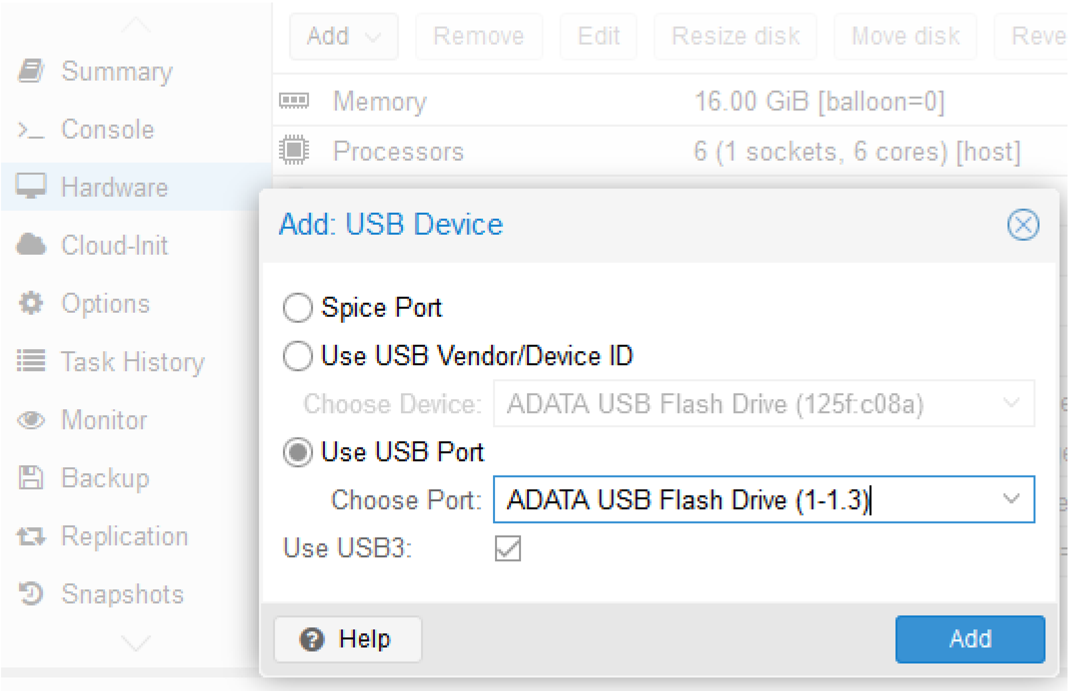
Choose Device: ADATA USB Flash Drive (125f:c08a)

○ Use USB Port

Choose Port: Passthrough a full port

Use USB3: ☑

    b. To add a flash drive using a USB port, select **Use USB Port**, and choose a port.



Memory 16.00 GiB [balloon=0]

Processors 6 (1 sockets, 6 cores) [host]

Add: USB Device

○ Spice Port

○ Use USB Vendor/Device ID

Choose Device: ADATA USB Flash Drive (125f:c08a)

● Use USB Port

Choose Port: ADATA USB Flash Drive (1-1.3)

Use USB3: ☑

5. Select **Add**.
6. Start the virtual machine.

Set Up the Virtual Appliance to Accept USB Flash Drives on an Operational VM - Proxmox VE Procedure

Before You Begin

Prepare the Virtual Appliance to accept USB flash drives.

1. Format the flash drive to FAT32.
2. Insert the flash drive into a USB port on the host.

Note
A USB device is required to be plugged in before it can be added to a virtual machine.

About This Task

The Virtual Appliance can accept USB flash drives. The flash drive can be used for backing up, restoring, upgrading, and collecting log information. A USB drive can be inserted, assigned to a virtual appliance, and removed from the virtual appliance while the appliance is in service.

To set up the VM to accept an USB flash drive when it is operational:

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Monitor**.
4. In the CLI, type **`info usbhost`** to display the list of USB devices available on the host.

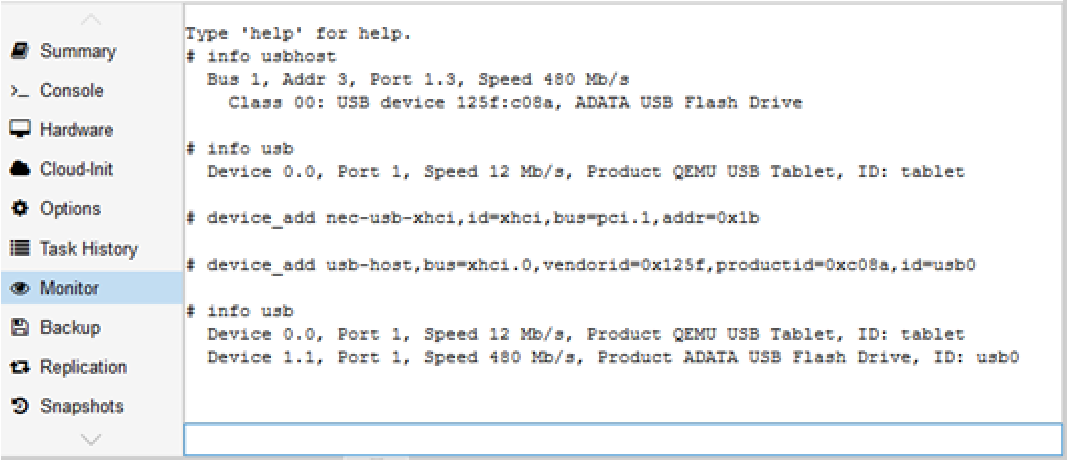
5. Type the following commands:

   `device_add nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b`

   `device_add usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0`

   Note
   The **vendorid** and **productid** arguments need to match the flash drive vendor or device ID from the info usbhost output.

   Adjust the **addr** field depending on the devices already defined on the PCI bus.



```
Type 'help' for help.
# info usbhost
  Bus 1, Addr 3, Port 1.3, Speed 480 Mb/s
    Class 00: USB device 125f:c08a, ADATA USB Flash Drive

# info usb
  Device 0.0, Port 1, Speed 12 Mb/s, Product QEMU USB Tablet, ID: tablet

# device_add nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b

# device_add usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0

# info usb
  Device 0.0, Port 1, Speed 12 Mb/s, Product QEMU USB Tablet, ID: tablet
  Device 1.1, Port 1, Speed 480 Mb/s, Product ADATA USB Flash Drive, ID: usb0
```

6. Type **`info usb`** to verify that the USB device was properly attached to the VM.

Manage the Flash Memory

About This Task

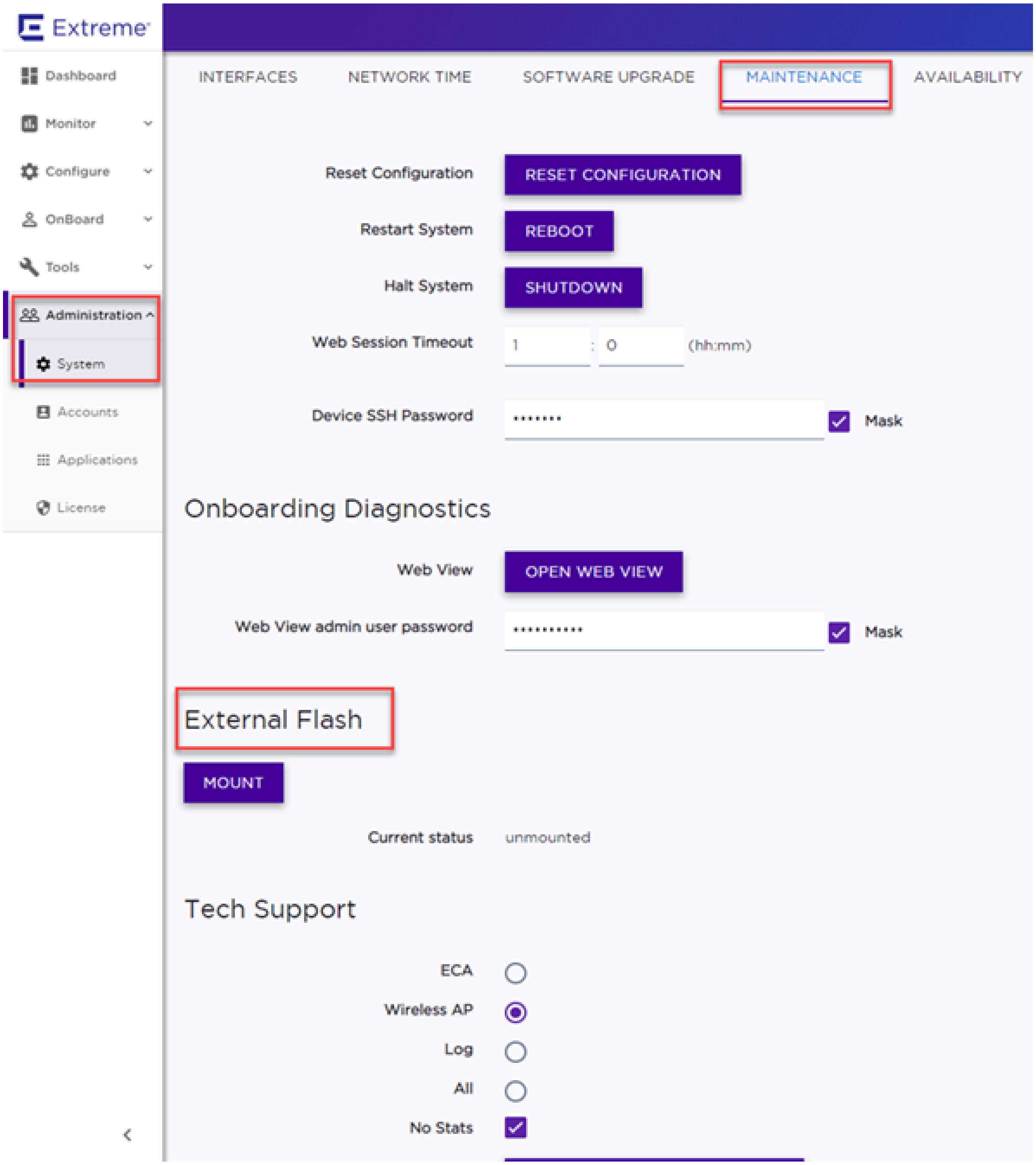
Follow these steps to manage flash memory:

Procedure

1. Log into the Extreme Campus Controller using your credentials.

2. In the left pane, from the **Administration** drop-down, select **System > Maintenance > External Flash** option.

   Use the **Mount/Unmount** options to mount and unmount flash memory respectively.



Reset Configuration

Restart System

Halt System

Web Session Timeout 1 : 0 (hh:mm)

Device SSH Password •••••••• ☑ Mask

Onboarding Diagnostics

Web View

Web View admin user password ••••••••••• ☑ Mask

External Flash

Current status unmounted

Tech Support

ECA ○

Wireless AP ●

Log ○

All ○

No Stats ☑

Figure 4: Flash memory maintenance window

Remove the Flash Drive - Generic Procedure

Before You Begin

When you are ready to remove the USB Flash drive, select **Un-Mount** from the Maintenance page.

About This Task

Follow these steps to remove the flash drive.

> Note
> The Virtual Appliance can be in service when the USB flash drive is assigned to it. Within a few seconds of the USB flash drive being assigned to it, the virtual appliance will detect the flash drive and mount it for use.

Procedure

1. Shut down the virtual machine.
2. Remove the USB device related configuration that was added to the virtual machine.

   For example:

   ```
   -device 'nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b'
   -device 'usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0'
   ```
3. Start the virtual machine.

   The USB flash drive can be removed from the host.

Remove the Flash Drive from a Proxmox VE Shutdown VM

Before You Begin

When you are ready to remove the USB Flash drive, select **Un-Mount** from the Maintenance page.

About This Task

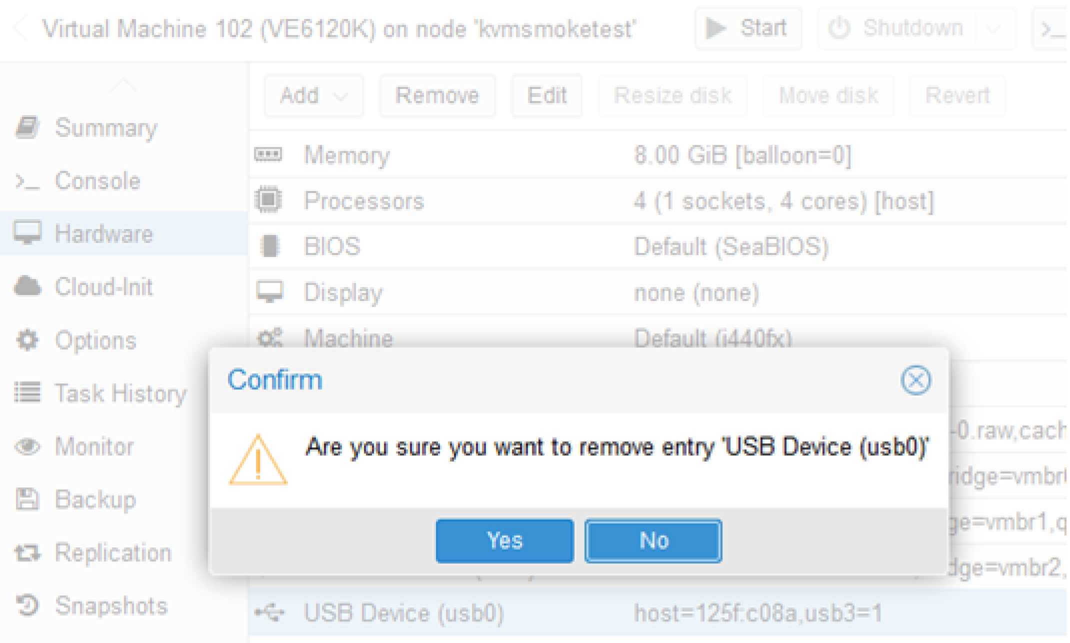
Follow these steps to remove the flash drive.

> Note
> The Virtual Appliance can be in service when the USB flash drive is assigned to it. Within a few seconds of the USB flash drive being assigned to it, the virtual appliance will detect the flash drive and mount it for use.

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Hardware**.
4. Select the corresponding USB device in the device list.
5. Select **Remove**.

6. Select **Yes** to confirm.



Virtual Machine 102 (VE6120K) on node 'kvmsmoketest'

Memory	8.00 GiB [balloon=0]
Processors	4 (1 sockets, 4 cores) [host]
BIOS	Default (SeaBIOS)
Display	none (none)
Machine	Default (i440fx)
USB Device (usb0)	host=125f:c08a,usb3=1

Are you sure you want to remove entry 'USB Device (usb0)'

The USB flash drive can be removed from the host.

Remove the Flash Drive from a Proxmox VE Operational VM

Before You Begin

When you are ready to remove the USB Flash drive, select **Un-Mount** from the Maintenance page.

About This Task

Follow these steps to remove the flash drive.

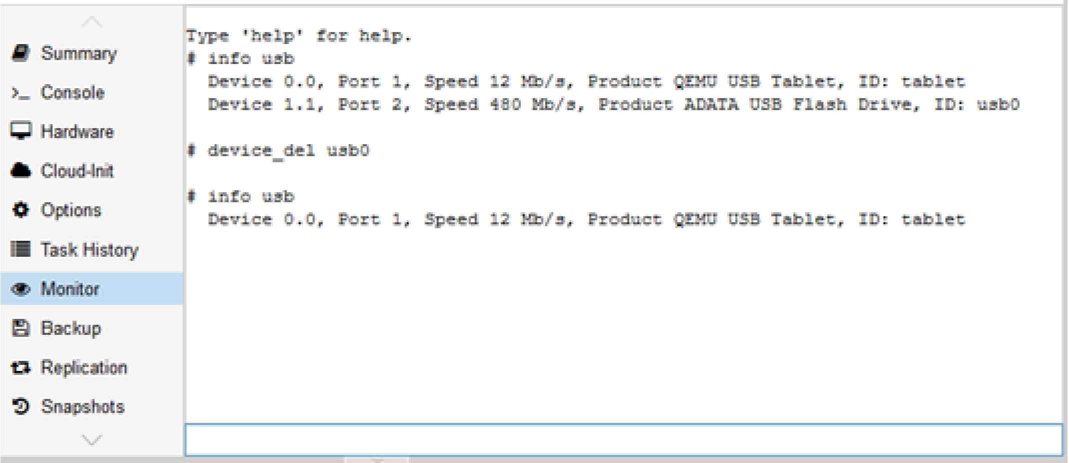
Note

The Virtual Appliance can be in service when the USB flash drive is assigned to it. Within a few seconds of the USB flash drive being assigned to it, the virtual appliance will detect the flash drive and mount it for use.

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Monitor**.

4. In the CLI, type **info usb** to display the list of attached USB devices.



```
Type 'help' for help.
# info usb
  Device 0.0, Port 1, Speed 12 Mb/s, Product QEMU USB Tablet, ID: tablet
  Device 1.1, Port 2, Speed 480 Mb/s, Product ADATA USB Flash Drive, ID: usb0

# device_del usb0

# info usb
  Device 0.0, Port 1, Speed 12 Mb/s, Product QEMU USB Tablet, ID: tablet
```

5. Type **device_del usb0**, where usb0 is the ID of the device that needs to be removed.

   The USB flash drive can be removed from the host.

Generate and Install the Activation Package

How to generate and install an Activation Package.

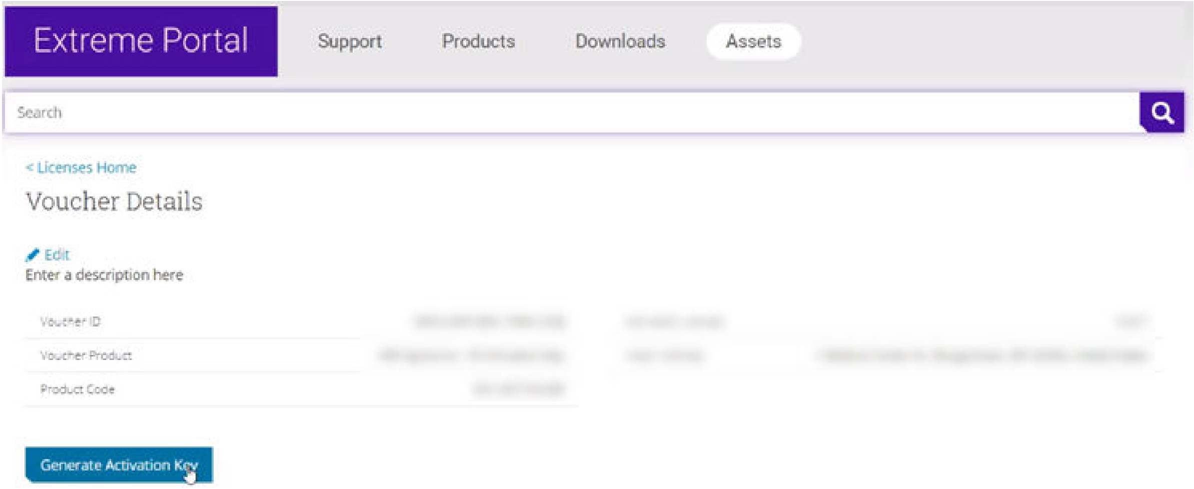
About This Task

All customers must generate and install an Activation Package for Extreme Campus Controller. Regardless of whether you obtain a new license or upgrade to Extreme Campus Controller. Take the following steps to generate and install the Activation Package:

Procedure

1. Log in to Extreme Campus Controller
2. Go to **Administration** > **License** to obtain the system **Locking ID**.
3. Log into the Extreme Support Portal: https://extremeportal.force.com/ExtrSupportHome.
4. Go to **Assets** > **Licenses Home** and select the Extreme Campus Controller Voucher ID line item from the list.

5. On the **Voucher Details** page, select **Generate Activation Key**.



Voucher Details

Enter a description here

Voucher ID	[redacted]	[redacted]	[redacted]
Voucher Product	[redacted]	[redacted]	[redacted]
Product Code	[redacted]		

Figure 5: Generate Activation Key

6. Provide the Locking ID for the Extreme Campus Controller that will be activated.
7. Check the box to accept **Terms and Conditions** and select **Submit**.
8. The Activation package is generated, and the **Save As** dialogue displays.
9. Download the Activation Package to your local machine.

> Note
> The Activation Package *file name* includes the Locking ID for the specific Extreme Campus Controller.

Install the Activation Package

About This Task

Stage your Extreme Campus Controller instance. Install the Activation Package to activate Extreme Campus Controller:

Procedure

1. Return to the Extreme Campus Controller instance from where you obtained the Locking ID.
2. Go to **Administration** > **License**.
3. Select the plus sign next to the **Activation License** field.
4. Drag the Activation Package to the **Upload License** dialog to install the Activation Package.

What to Do Next

For more information on licensing, refer to the Extreme Campus Controller User Guide.

Related Topics

Subscription License on page 46

Permanent Capacity License on page 46

Subscription License

Learn about Subscription Licensing.

Subscription licensing is available for Extreme Campus Controller for both access point and switch management. Upon purchase of a new Extreme Campus Controller you will receive a welcome email and activation instructions.

Each appliance obtains capacity Right to Use (RTU) entitlements regarding managed devices, subject to the system limits of the appliance instance and the total number of activations purchased. The total consumed RTU across all Extreme Campus Controller instances cannot exceed the number of RTU you have subscribed to. Each appliance provides visualization on specific RTU allocation and overall balance. For subscription management, Extreme Campus Controller requires a configured DNS server and constant connection to the Internet in order to be operational.

Note

Extreme Campus Controller must access the License Server (cloud-based service).

The controller's DNS server configuration must facilitate resolution of the URL: https://prod.extreme.sentinelcloud.com/productConnector/. When there is a firewall in place, it must allow access to that service (HTTPS = TCP 443).

Related Topics

Generate and Install the Activation Package on page 44

Permanent Capacity License

Learn about a Capacity License.

About This Task

A Permanent Capacity License is offered with a permanent activation, and it works with a separate capacity key. The alternative to a Permanent Capacity License is a Subscription License. The activation process is the same regardless of the license model you choose.

The Extreme Campus Controller Permanent Capacity License works on simple software-based key strings. A key string consists of a series of numbers and/or letters. Using these key strings, you can enhance the capacity of the controller to manage additional APs.

Note

The controller does not require internet access with Permanent Capacity Licensing.

- Capacity key — Enhances the capacity of the appliance to manage devices. Extreme Campus Controller supports capacity enhancement keys for 5, 25, 100, 500 or 2000 APs. Max capacity on an Extreme Campus Controller instance is subject to the appliance type and the capacity tier configured (based on hypervisor resources for Virtual instances).

  Capacity applies to all managed devices (access points and switches). A capacity license is shared between nodes in an Availability Pair. Install the capacity license on only one of the nodes in the

Availability Pair. Extreme Campus Controller and availability pair will restrict the user from installing the same capacity key again if it exists on either appliance.

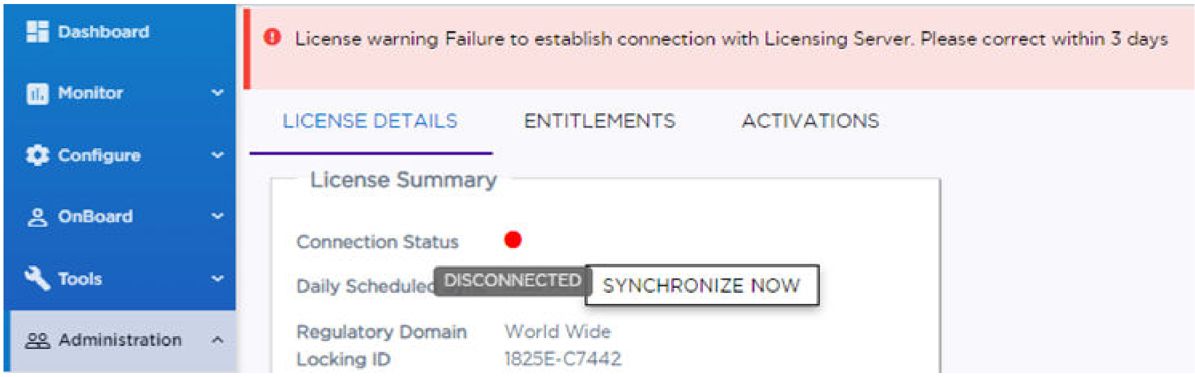
Note
A capacity license cannot be installed on an Extreme Campus Controller if its peer has the same capacity key applied.

To obtain a Permanent Capacity License:

Procedure

1. Go to the Support portal to generate an Activation Package. For more information, see Generate and Install the Activation Package on page 44.
2. From the Support portal, obtain your capacity keys. For more information, see Obtain and Apply a Capacity Key on page 48.

   There is no connection to the licensing server when an Activation Package for Permanent Capacity Licensing is installed. Therefore, the Extreme Campus Controller displays a connection failure message. This message can be ignored for Permanent Capacity Licensing. Simply select the **Switch to Permanent Licensing** link to clear the message.



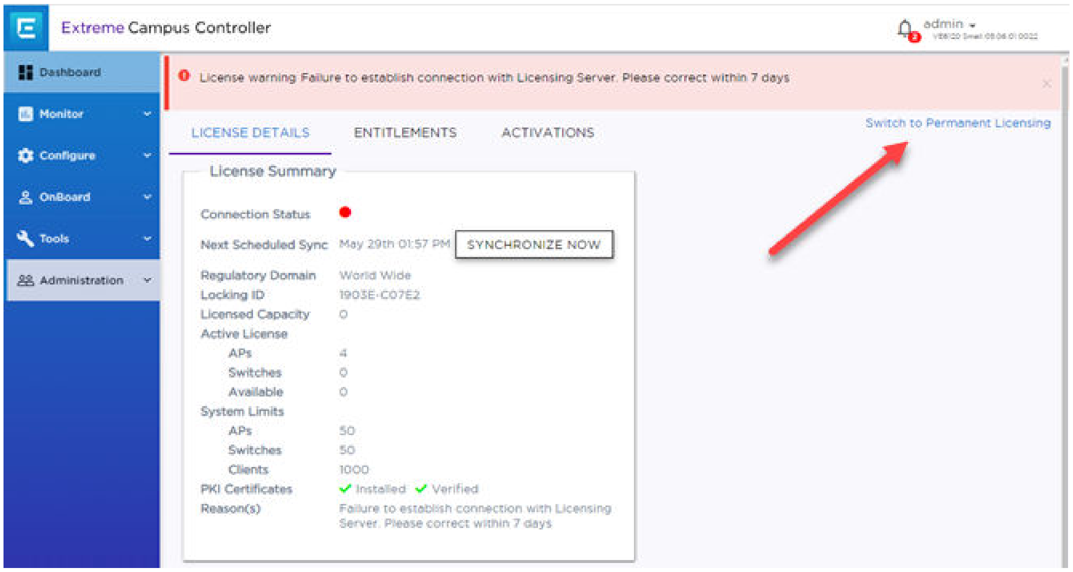
License warning Failure to establish connection with Licensing Server. Please correct within 3 days

License Summary

Connection Status ●
Daily Scheduled
Regulatory Domain World Wide
Locking ID 1825E-C7442

Figure 6: Connection to License Server message when Permanent Licensing is applied

3. After selecting **Switch to Permanent Licensing**, your valid capacity limits are displayed.



License warning Failure to establish connection with Licensing Server. Please correct within 7 days

License Summary

Connection Status	●
Next Scheduled Sync	May 29th 01:57 PM
Regulatory Domain	World Wide
Locking ID	1903E-C07E2
Licensed Capacity	0
Active License	
APs	4
Switches	0
Available	0
System Limits	
APs	50
Switches	50
Clients	1000
PKI Certificates	✓ Installed ✓ Verified
Reason(s)	Failure to establish connection with Licensing Server. Please correct within 7 days

Figure 7: Switch to Permanent Capacity Licensing

Related Topics

Generate and Install the Activation Package on page 44

Obtain and Apply a Capacity Key

About This Task

Procedure

1. Obtain a voucher from the Extreme Networks Support portal.
2. Log into the Extreme Networks Support portal to redeem the voucher.

   The Extreme Networks Support portal presents the Capacity key.
3. On the Extreme Campus Controller, go to **Administration** > **License**.
4. Select the **Permanent Capacity License** link.
5. Next to the **Licensed Capacity** field, select the plus sign.
6. Copy and paste the Capacity key from the Extreme Networks Support portal to the Extreme Campus Controller user interface.
7. Select **Apply**.

Results

Note
When using a Permanent Capacity License model, on Extreme Campus Controller, select the **Permanent Capacity License** link. Your valid capacity limits are now displayed.

Shut Down and Restart a Virtual Machine

About This Task

The following task will outline the various ways through which you can shut down and reboot a virtual machine.

For information on how to access the Basic Configuration Wizard, see Access the Virtual Appliance Console on page 29.

To shut down and reboot the virtual machine using the Command Line Interface (CLI) in the Basic Configuration Wizard:

Procedure

1. Type `shutdown halt` and press **Enter** in the Basic Configuration Wizard.

   The virtual machine shuts down.
2. To reboot the virtual machine, type `shutdown reboot` and press **Enter**.

   The virtual machine restarts.

Shut Down and Restart a Virtual Machine Using the Graphical User Interface (GUI)

About This Task

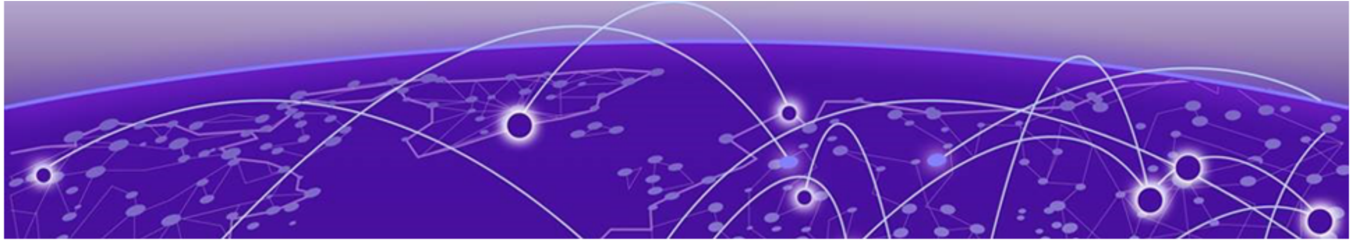
To shut down and restart a virtual machine using the GUI:

Procedure

1. Navigate to **Administration** > **System** > **Maintenance**.
2. Select **Halt System (SHUTDOWN)**.

   The machine shuts down.
3. To restart the machine, select **Restart System (REBOOT)**.

   The machine restarts.



Configure Bridges for the Virtual Appliance

The Virtual Appliance has some specific requirements on the bridges to which its data plane ports are connected. The following section explains how to create a bridge on a host that satisfies these requirements.

Create a New Bridge on the KVM Server - Generic Procedure

About This Task

This is an optional step since it is possible to reconfigure an existing bridge on the host. However, using separate bridge for the data plane traffic helps to isolate that traffic from other virtual devices.

To create a new bridge using the generic procedure:

Procedure

Create a Linux bridge attached to the desired network device.

Example:

```
iface ens3f0 inet manual

         auto vmbr1
         iface vmbr1 inet manual
               bridge-ports ens3f0
               bridge-stp off
               bridge-fd 0
```

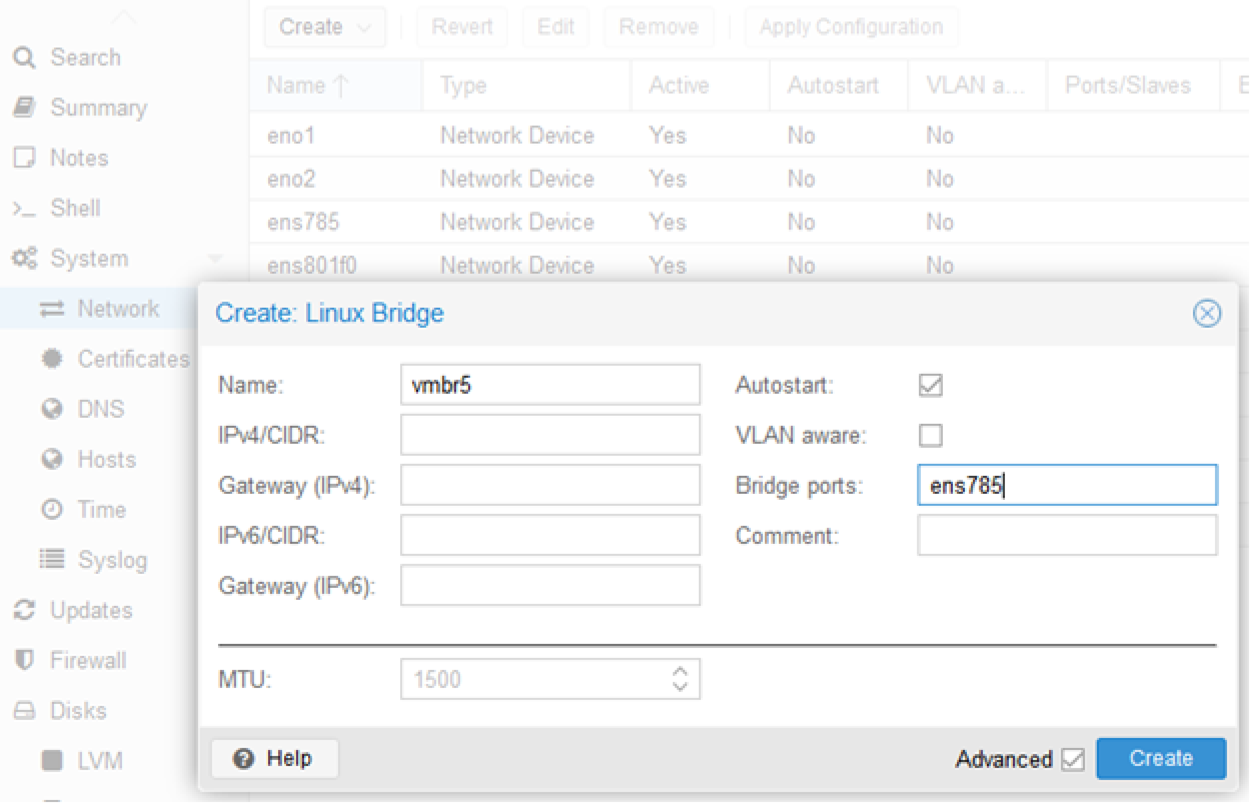
Create a New Bridge on the KVM Server - Proxmox VE Procedure

About This Task

To create a new bridge using the Proxmox VE procedure:

Procedure

1. Log into the Proxmox GUI.
2. In the left pane, select the KVM server host name.
3. Select **System** > **Network**
4. Select **Create**.
5. Select **Linux Bridge** from the drop-down list.



Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	E
eno1	Network Device	Yes	No	No		
eno2	Network Device	Yes	No	No		
ens785	Network Device	Yes	No	No		
ens801f0	Network Device	Yes	No	No		

Create: Linux Bridge

Name:	vmbr5	Autostart:	☑
IPv4/CIDR:		VLAN aware:	☐
Gateway (IPv4):		Bridge ports:	ens785
IPv6/CIDR:		Comment:	
Gateway (IPv6):			
MTU:	1500		

Advanced ☑

Figure 8: Create Linux Bridge window

6. Set a Linux bridge name.
7. Set a bridge ports name that matches the network device name of the bridge.
8. Select **Create**.

Configure the Bridge for Jumbo Frames Support - Generic Procedure

About This Task

The jumbo frames feature enables the configuration of physical Maximum Transmission Unit (MTU) sizes up to 1800 bytes on the access point and appliance Ethernet data plane ports. The Admin port, all protocols, and interfaces continue to use the standard MTU size of 1500 bytes.

Enable Jumbo Frames to facilitate the transmission of MU data between the access point and the appliance, or between the access point and a bridge for VxLAN topologies, without incurring fragmentation.

To configure the bridge for jumbo frames support using the generic procedure:

Procedure

Set the MTU of the network devices and the data plane ports attached bridges to 1800.

Configure the Bridge for Jumbo Frames Support - Proxmox VE Procedure

About This Task

The jumbo frames feature enables the configuration of physical Maximum Transmission Unit (MTU) sizes up to 1800 bytes on the access point and appliance Ethernet data plane ports. The Admin port, all protocols, and interfaces continue to use the standard MTU size of 1500 bytes.

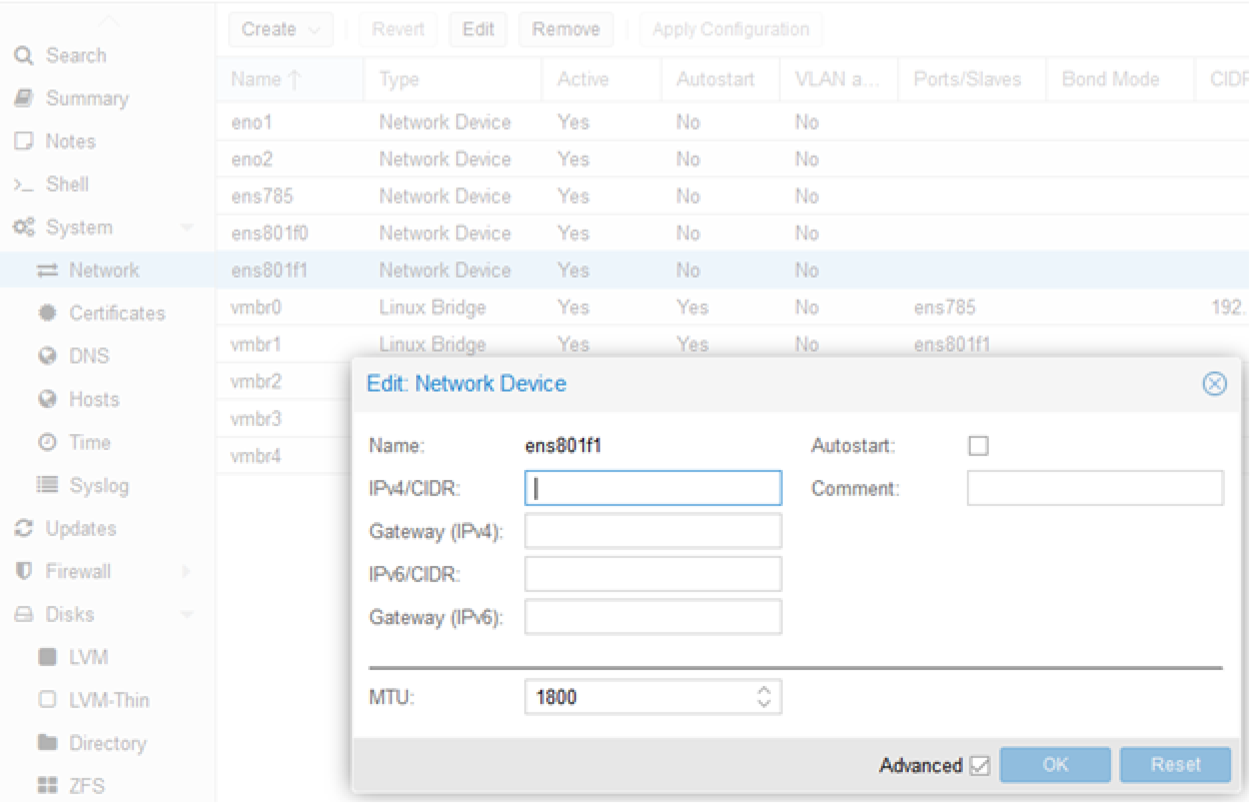
Enable Jumbo Frames to facilitate the transmission of MU data between the access point and the appliance, or between the access point and a bridge for VxLAN topologies, without incurring fragmentation.

To configure the bridge for jumbo frames support using the Proxmox VE procedure:

Procedure

1. In the left pane, select the VM from the KVM server host name.
2. Select **System** > **Network**.
3. Select the network device that must be configured.
4. Select **Edit**.

Figure 9: Network device edit window



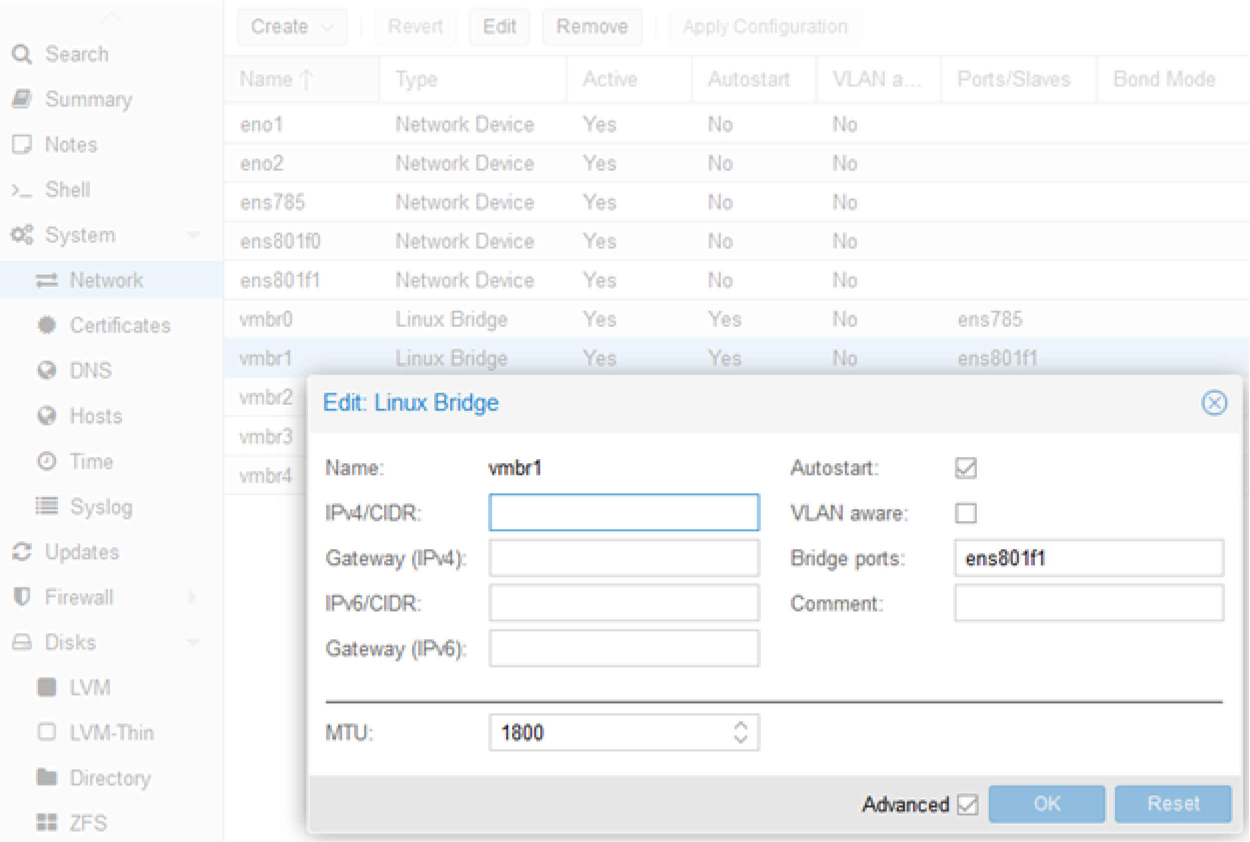
Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDF
eno1	Network Device	Yes	No	No			
eno2	Network Device	Yes	No	No			
ens785	Network Device	Yes	No	No			
ens801f0	Network Device	Yes	No	No			
ens801f1	Network Device	Yes	No	No			
vmbr0	Linux Bridge	Yes	Yes	No	ens785		192.
vmbr1	Linux Bridge	Yes	Yes	No	ens801f1		
vmbr2							
vmbr3							
vmbr4							

Edit: Network Device

Name: ens801f1
IPv4/CIDR:
Gateway (IPv4):
IPv6/CIDR:
Gateway (IPv6):
Autostart: □
Comment:
MTU: 1800

Advanced ☑ OK Reset

5. Set the MTU value to 1800.
6. Select **OK**.
7. Select the Linux bridge attached to the corresponding network device.
8. Select **Edit**.



Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode
eno1	Network Device	Yes	No	No		
eno2	Network Device	Yes	No	No		
ens785	Network Device	Yes	No	No		
ens801f0	Network Device	Yes	No	No		
ens801f1	Network Device	Yes	No	No		
vmbr0	Linux Bridge	Yes	Yes	No	ens785	
vmbr1	Linux Bridge	Yes	Yes	No	ens801f1	
vmbr2						
vmbr3						
vmbr4						

Edit: Linux Bridge

Name: vmbr1
IPv4/CIDR:
Gateway (IPv4):
IPv6/CIDR:
Gateway (IPv6):
Autostart: ☑
VLAN aware: ☐
Bridge ports: ens801f1
Comment:
MTU: 1800
Advanced ☑ OK Reset

Figure 10: Linux bridge edit window

9. Set the MTU value to 1800.
10. Select **OK**.

Index